

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 9 月 5 日

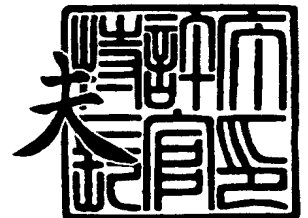
出 願 番 号
Application Number: 特 願 2 0 0 3 - 3 1 4 4 6 4
[ST. 10/C]: [J P 2 0 0 3 - 3 1 4 4 6 4]

出 願 人
Applicant(s): 株式会社リコー

2 0 0 3 年 1 0 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 0304084
【提出日】 平成15年 9月 5日
【あて先】 特許庁長官 今井 康夫 殿
【国際特許分類】 G06F 12/00 537
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 斉藤 敦久
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 金井 洋一
【発明者】
 【住所又は居所】 東京都大田区中馬込 1 丁目 3 番 6 号 株式会社リコー内
 【氏名】 谷内田 益義
【特許出願人】
 【識別番号】 000006747
 【氏名又は名称】 株式会社リコー
【代理人】
 【識別番号】 100070150
 【弁理士】
 【氏名又は名称】 伊東 忠彦
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-273985
 【出願日】 平成14年 9月19日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-275973
 【出願日】 平成14年 9月20日
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-297888
 【出願日】 平成14年10月10日
【手数料の表示】
 【予納台帳番号】 002989
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9911477

【書類名】 特許請求の範囲**【請求項 1】**

ドキュメントの識別情報を読み取る識別情報読取手段と、
上記識別情報によって指定される動作要件を選択する動作要件選択手段と、
上記動作要件選択手段によって選択された1つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有することを特徴とする画像形成装置。

【請求項 2】

前記動作要件は、上記ドキュメントに対するセキュリティに関する要件であることを特徴とする請求項 1 記載の画像形成装置。

【請求項 3】

上記所定動作は、電子データで画像を形成することを特徴とする請求項 1 又は 2 記載の画像形成装置。

【請求項 4】

上記所定動作は、上記ドキュメントを用紙上に印刷することを特徴とする請求項 1 又は 2 記載の画像形成装置。

【請求項 5】

上記識別情報読取手段は、
上記ドキュメントに対する所定読み取り動作によって取得したデータを上記識別情報として認識する識別情報認識手段と、
上記識別情報とドキュメント属性とを対応付けして管理するドキュメント属性管理手段と、
ドキュメント属性管理手段を参照することによって、上記識別情報認識手段によって認識された上記識別情報に対応する上記ドキュメント属性を取得するドキュメント属性取得手段とを有することを特徴とする請求項 1 乃至 4 のいずれか一項記載の画像形成装置。

【請求項 6】

上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントに印字されたバーコード、二次元コード又は磁気コード、又は、該ドキュメントに付与された R F I D のいずれかを読み取って上記識別情報として認識することを特徴とする請求項 5 記載の画像形成装置。

【請求項 7】

上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントを読み取って生成される電子画像データから、バーコード、二次元コード、数字情報、文字情報、ドットパターンのいずれかを上記識別情報として認識することを特徴とする請求項 5 記載の画像形成装置。

【請求項 8】

上記所定動作を要求するユーザに関するユーザ属性を取得するユーザ属性取得手段を更に有することを特徴とする請求項 1 乃至 7 のいずれか一項記載の画像形成装置。

【請求項 9】

上記ユーザ属性取得手段は、
上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、
該ユーザ識別情報と上記ユーザ属性とを対応付けして管理するユーザ属性管理手段と、
上記ユーザ識別情報に基づいて上記ユーザを認証するユーザ認証手段と、
上記ユーザ認証手段による認証結果に基づいて、上記ユーザ属性管理手段を参照することによって、上記ユーザ識別情報取得手段によって取得された上記ユーザ識別情報に対応する上記ユーザ属性を取得するユーザ属性取得手段とを有することを特徴とする請求項 8 記載の画像形成装置。

【請求項 10】

上記ユーザ属性取得手段は、
上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段

と、

上記ユーザを認証し、上記ユーザ属性を提供する外部サーバに対して該ユーザ属性を要求するユーザ属性要求手段とを有することを特徴とする請求項 8 記載の画像形成装置。

【請求項 1 1】

上記動作要件が実行可能であるか否かを判断する動作要件判断手段と、

上記動作要件判断手段による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手段とを有することを特徴とする請求項 1 乃至 1 0 のいずれか一項記載の画像形成装置。

【請求項 1 2】

上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、電子透かしを埋め込むことを指示することを特徴とする請求項 1 乃至 1 1 のいずれか一項記載の画像形成装置。

【請求項 1 3】

上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、表示可能なラベルを埋め込むことを指示することを特徴とする請求項 1 乃至 1 1 のいずれか一項記載の画像形成装置。

【請求項 1 4】

上記表示可能なラベルは、少なくとも上記所定動作を要求したユーザの認証データと、上記所定動作を要求した時点のタイムスタンプを含むことを特徴とする請求項 9 乃至 1 1 のいずれか一項記載の画像形成装置。

【請求項 1 5】

上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、少なくとも上記所定動作を要求したユーザの認証データと、該所定動作によって生成される上記ドキュメントのドキュメントデータと、読み取りを指示した時点のタイムスタンプとをログに記録することを特徴とする請求項 9 乃至 1 1 のいずれか一項記載の画像形成装置。

【請求項 1 6】

上記ドキュメントのネットワーク配信を可能とする上記動作要件を満たしつつ上記所定動作が実行し、実行によって生成されたドキュメントデータをネットワークを介して配信する配信手段を有することを特徴とする請求項 1 乃至 1 5 のいずれか一項記載の画像形成装置。

【請求項 1 7】

ドキュメントの識別情報を読み取る識別情報読取手順と、

上記識別情報によって指定される動作要件を選択する動作要件選択手順と、

上記動作要件選択手順によって選択された 1 つ以上の動作要件に従って所定動作の実行を制御する動作制御手順とを有することを特徴とする画像形成方法。

【請求項 1 8】

上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、

上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手順とを有することを特徴とする請求項 1 7 記載の画像形成方法。

【請求項 1 9】

ドキュメントの識別情報を読み取る識別情報読取手順と、

上記識別情報によって指定される動作要件を選択する動作要件選択手順と、

上記動作要件選択手順によって選択された 1 つ以上の動作要件に従って所定動作の実行を制御する動作制御手順と、

上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、

上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手順とをコンピュータに実行させることを特徴とするコンピュータ実行可能なプログラム。

【請求項 2 0】

ドキュメントの識別情報を読み取る識別情報読取手順と、
上記識別情報によって指定される動作要件を選択する動作要件選択手順と、
上記動作要件選択手順によって選択された1つ以上の動作要件に従って所定動作の実行
を制御する動作制御手順と、
上記動作要件が実行可能であるか否かを判断する動作要件判断手順と、
上記動作要件判断手順による判断結果が上記動作要件が実行可能でないことを示す場合
、上記所定動作を禁止する動作禁止手順とをコンピュータに実行させることを特徴とする
プログラムが記憶されたコンピュータ読み取り可能な記憶媒体。

【書類名】明細書**【発明の名称】情報処理装置及び情報処理方法****【技術分野】****【0001】**

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法に関連する。

【背景技術】**【0002】**

オフィスに代表されるようなドキュメントを扱うフィールドでは、そのドキュメントのセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等、特に情報のコンテナであるドキュメントに対するポリシー、中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【0003】

現実には多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【0004】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献1から、特許文献14）。

【0005】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献1）。

【0006】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている（特許文献2）。

【0007】

しかし、特に、上述の特許文献1では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【0008】

また、上述の特許文献2では、セキュリティポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるDB（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【0009】

また、特許文献7の操作者IDを入力させ、文書からIDを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。

【0010】

特許文献8の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うか否かが決められているため、ルールの柔軟性に欠ける。

【0011】

特許文献 9 の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【0012】

特許文献 10 の画像を読み取ってパスワードとともに記憶し、出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【0013】

特許文献 11 のネットワーク上の複数の MFP のうち、一つの MFP がユーザ管理を行ってネットワーク上の MFP すべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【0014】

特許文献 12 の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可、不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」の ID に対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【特許文献 1】特開 2001-184264 号公報

【特許文献 2】特開 2001-273388 号公報

【特許文献 3】特開 2001-337864 号公報

【特許文献 4】特開平 09-293036 号公報

【特許文献 5】特開平 07-141296 号公報

【特許文献 6】特許第 02735966 号公報

【特許文献 7】特許 3203103 号公報

【特許文献 8】特開平 7-58950 号公報

【特許文献 9】特開平 7-152520 号公報

【特許文献 10】特開平 10-191072 号公報

【特許文献 11】特開 2000-15898 号公報

【特許文献 12】特開 2000-357064 号公報

【特許文献 13】特開 2001-125759 号公報

【特許文献 14】特開 2001-325249 号公報。

【発明の開示】

【発明が解決しようとする課題】

【0015】

このようなセキュリティの実施方法では、ドキュメントの印刷に対するセキュリティを実行する場合には、第 1 に、セキュリティの施行者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第 2 には、すべての機器に対してセキュリティが、一つ一つ実行される必要がある。第 3 には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第 4 に、個々の機器にセキュリティが実施されていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。

【0016】

本発明は、上述の問題点を解決することを目的とする。

【0017】

特に本発明の目的は、ドキュメントに関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う画像形成装置、その画像形成装置での処理を実行するプログラム、及び、そのプログラムを記憶した記憶媒体を提供することである。

【課題を解決するための手段】

【0018】

上記課題を解決するため、本発明は、請求項1に記載されるように、ドキュメントの識別情報を読み取る識別情報読取手段と、上記識別情報によって指定される動作要件を選択する動作要件選択手段と、上記動作要件選択手段によって選択された1つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有するように構成される。

【0019】

このような画像形成装置では、読み取った識別情報で動作要件（動作条件）を選択することができる。すなわち、紙のドキュメントに対して、例えば、組織のセキュリティポリシーに従った動作要件を満たすように印刷、コピー、FAX等を制御することができる。

【0020】

また、本発明は、請求項2に記載されるように、前記動作要件は、上記ドキュメントに対するセキュリティに関する要件であるように構成することができる。

【0021】

また、本発明は、請求項3に記載されるように、上記所定動作は、電子データで画像を形成するように構成することができる。

【0022】

また、本発明は、請求項4に記載されるように、上記所定動作は、上記ドキュメントを用紙上に印刷するように構成することができる。

【0023】

また、本発明は、請求項5に記載されるように、上記識別情報読取手段は、上記ドキュメントに対する所定読み取り動作によって取得したデータを上記識別情報として認識する識別情報認識手段と、上記識別情報とドキュメント属性とを対応付けして管理するドキュメント属性管理手段と、ドキュメント属性管理手段を参照することによって、上記識別情報認識手段によって認識された上記識別情報に対応する上記ドキュメント属性を取得するドキュメント属性取得手段とを有するように構成することができる。

【0024】

またセキュリティポリシー、本発明は、請求項6に記載されるように、上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントに印字されたバーコード、二次元コード又は磁気コード、又は、該ドキュメントに付与されたRFIDのいずれかを読み取って上記識別情報として認識するように構成することができる。

【0025】

また、本発明は、請求項7に記載されるように、上記所定読み取り動作は、上記ドキュメントが用紙である場合に、該ドキュメントを読み取って生成される電子画像データから、バーコード、二次元コード、数字情報、文字情報、ドットパターンのいずれかを上記識別情報として認識するように構成することができる。

【0026】

また、本発明は、請求項8に記載されるように、上記所定動作を要求するユーザに関するユーザ属性を取得するユーザ属性取得手段を更に有するように構成することができる。

【0027】

また、本発明は、請求項9に記載されるように、上記ユーザ属性取得手段は、上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、該ユーザ識別情報と上記ユーザ属性とを対応付けして管理するユーザ属性管理手段と、上記ユーザ識別情報に基づいて上記ユーザを認証するユーザ認証手段と、上記ユーザ認証手段による認証結果に基づいて、上記ユーザ属性管理手段を参照することによって、上記ユーザ識別情報取得手段によって取得された上記ユーザ識別情報に対応する上記ユーザ属性を取得するユーザ属性取得手段とを有するように構成することができる。

【0028】

また、本発明は、請求項10に記載されるように、上記ユーザ属性取得手段は、上記ユーザから該ユーザを識別するユーザ識別情報を取得するユーザ識別情報取得手段と、上記ユーザを認証し、上記ユーザ属性を提供する外部サーバに対して該ユーザ属性を要求するユーザ属性要求手段とを有するように構成することができる。

【0029】

また、本発明は、請求項11に記載されるように、上記動作要件が実行可能であるか否かを判断する動作要件判断手段と、上記動作要件判断手段による判断結果が上記動作要件が実行可能でないことを示す場合、上記所定動作を禁止する動作禁止手段とを有するように構成することができる。

【0030】

また、本発明は、請求項12に記載されるように、上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、電子透かしを埋め込むことを指示するように構成することができる。

【0031】

また、本発明は、請求項13に記載されるように、上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、表示可能なラベルを埋め込むことを指示するように構成することができる。

【0032】

また、本発明は、請求項14に記載されるように、上記表示可能なラベルは、少なくとも上記所定動作を要求したユーザの認証データと、上記所定動作を要求した時点のタイムスタンプを含むように構成することができる。

【0033】

また、本発明は、請求項15に記載されるように、上記動作要件は、上記ドキュメントに対する上記所定動作の実行の際に、少なくとも上記所定動作を要求したユーザの認証データと、該所定動作によって生成される上記ドキュメントのドキュメントデータと、読み取りを指示した時点のタイムスタンプとをログに記録するように構成することができる。

【0034】

また、本発明は、請求項16に記載されるように、上記ドキュメントのネットワーク配信を可能とする上記動作要件を満たしつつ上記所定動作が実行し、実行によって生成されたドキュメントデータをネットワークを介して配信する配信手段を有するように構成することができる。

【0035】

上記課題を解決するための手段として、本発明は、上記画像形成装置での処理をコンピュータに行なわせるための画像形成方法及びプログラム、及び、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体とすることもできる。

【発明の効果】**【0036】**

本願発明によれば、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法を提供することができる。

【発明を実施するための最良の形態】**【0037】**

以下、本発明の実施の形態を図面に基づいて説明する。

【0038】

本発明の実施例を、以下に詳細に説明する。

【0039】

本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（DSP）と呼ぶ。

【0040】

図1は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図1のようなセキュリティポリシーを掲げることが想定される。

【 0 0 4 1 】

このようなポリシーを D S P として記述できるようにするために、以下のような方法を使用する。

【 0 0 4 2 】

まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリー（人事文書、技術文書など）に応じて分類する。この、機密レベルとカテゴリーの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。

【 0 0 4 3 】

上記のような、分類の仕方の一例を図 2 に示す。図 2 は、ドキュメントラベル用語ファイルの例を示す。図 2 に示されるようなドキュメントラベル用語ファイル 3 0 0 は、個々のドキュメントに属性情報として付与されるラベルのリストを管理するファイルであり、例えば、XML によって記述される。

【 0 0 4 4 】

D S P には、ドキュメントの機密レベル及びカテゴリーに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリーを記述するのが、図 2 のドキュメントラベル用語ファイル 3 0 0 である。

【 0 0 4 5 】

図 2 において、<enumeration>から</enumeration>で示される記述 3 1 1 及び記述 3 2 1 によって、2 種類のカテゴリーが示される。

【 0 0 4 6 】

記述 3 1 1 において、<enum_id>doc_category</enum_id>を示す記述 3 1 2 は、カテゴリーの識別情報が「doc_category」であることを示す。<enum_name>Document Category</enum_name>を示す記述 3 1 3 は、カテゴリーの名称が「Document Category」であることを示す。<description>文書カテゴリーの種類</description>を示す記述 3 1 4 は、このカテゴリーが何を分類するか示す説明「文書カテゴリーの種類」を示す。

【 0 0 4 7 】

<item>から</item>を示す記述 3 1 5、記述 3 1 6 及び記述 3 1 7 によって、3 つのカテゴリーの項目が示される。記述 3 1 5 は、<name>internal_doc</name>を示す記述によって、項目名が「internal_doc」であることを示し、<description>社内一般文書</description>を示す記述によって、その項目の説明「社内一般文書」を示す。

【 0 0 4 8 】

記述 3 1 6 は、<name>human_resource_doc</name>を示す記述によって、項目名が「human_resource_doc」であることを示し、<description>人事関連文書</description>を示す記述によって、その項目の説明「人事関連文書」を示す。

【 0 0 4 9 】

記述 3 1 7 は、<name>technical_doc</name>を示す記述によって、項目名が「technical_doc」であることを示し、<description>技術関連文書</description>を示す記述によって、その項目の説明「技術関連文書」を示す。

【 0 0 5 0 】

同様に、記述 3 2 1 において、<enum_id>doc_security_level</enum_id>を示す記述 3 2 2 は、カテゴリーの識別情報が「doc_security_level」であることを示す。<enum_name>Document Security Level</enum_name>を示す記述 3 2 3 は、カテゴリーの名称が「Document Security Level」であることを示す。<description>文書のセキュリティレベルの種類</description>を示す記述 3 2 4 は、このカテゴリーが何を分類するか示す説明「文書のセキュリティレベルの種類」を示す。

【 0 0 5 1 】

<item>から</item>を示す記述 3 2 5、記述 3 2 6 及び記述 3 2 7 によって、3 つの

テゴリーの項目が示される。記述 325 は、<name>basic</name>を示す記述によって、項目名が「basic」であることを示し、<description>社外秘</description>を示す記述によって、その項目の説明「社外秘」を示す。

【0052】

記述 326 は、<name>medium</name>を示す記述によって、項目名が「medium」であることを示し、<description>秘</description>を示す記述によって、その項目の説明「秘」を示す。

【0053】

記述 327 は、<name>high</name>を示す記述によって、項目名が「high」であることを示し、<description>極秘</description>を示す記述によって、その項目の説明「極秘」を示す。

【0054】

このように、ドキュメントラベル用語ファイル 300 によって、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリーの種類が規定される。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が規定される。

【0055】

図 3 から図 13 は、ポリシー用語ファイルの例を示す図を示す。図 3 から図 13 により、1 つのポリシー用語ファイル 400 を構成する。

【0056】

図 3 から図 13 に示されるようなポリシー用語ファイル 400 は、システムタイプの分類を記述し、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。ポリシー用語ファイル 400 は、例えば、XML によって記述される。

【0057】

図 3 において、列挙して記述する方法は、図 2 に示すドキュメントラベルファイル 300 での記述方法と同様に<enumeration>から</enumeration>までの記述を繰り返すことによって示される。<enumeration>から</enumeration>までの詳細な記述は、図 2 に示すドキュメントラベルファイル 300 での記述方法と同様であるので、ここでは、簡単な説明のみとする。

【0058】

例えば、図 3 においては、記述 411 によってシステムタイプが列挙される。記述 411 によると、「システムタイプの種類」として、「複写機」、「プリンタ」、「ファクシミリ」、「スキャナ」、「文書リポジトリ」、及び、「電子会議システム」が記述される。

【0059】

そして、例えば、図 4 に示されたように、記述 421 から記述 471 によってシステムタイプごとの各オペレーションが列挙される。

【0060】

記述 421 において、「複写機に関わるオペレーション」として、「紙から紙への複写」が記述される。記述 431 において、「プリンタに係わるオペレーション」として、「電子文書を紙へ印刷」が記載される。記述 441 において、「ファックスに関わるオペレーション」として、「ファックス送信」及び「ファックス受信」が記載される。記述 451 において、「スキャナに関わるオペレーション」として、「紙文書をスキャンして電子文書にする」が記載される。

【0061】

記述 461 において、「文書リポジトリに関わるオペレーション」として、「保存する」、「改訂・編集する」、「削除・破棄する」、「参照する」、「ネットワークで配布する（送信する）」、「ディスクで配布する（送付する）」、及び、「アーカイブ・バックアップする」が記述される。記述 471 において、「電子会議システムに関わるオペレーション」として、「会議で利用する」が記述される。

【0062】

更に、例えば、図6から図13示すように、記述481から記述601によってオペレーション毎に適用できる要件が列挙される。

【0063】

記述481において、「複写に関わる要件」として、「明示的な許可」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【0064】

記述491において、「印刷に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「プリントした本人による紙出力」、「信頼チャネルの利用（印刷データの暗号化）」、及び、「プリントアウトに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【0065】

記述501において、「ファックス送信に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「宛先制限」、「親展モードでの送信」、「信頼チャネルの利用」、「送信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」、及び、「否認防止（受取証の取得）」が記載される。

【0066】

記述511において、「ファックス受信に関わる要件」として、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「親展ファックスの宛先本人による取り出し」、「信頼タイムスタンプ」、及び、「受信ファックスに追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【0067】

記述521において、「スキャンに関わる要件（保存した後については保存要件を適用する）」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「スキャン画像に追跡情報埋め込み（透かし、ラベル、バーコード）」が記載される。

【0068】

記述531において、「保存に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「保存データの暗号化」、及び、「保存データの改ざん保護」が記載される。

【0069】

記述541において、「改訂に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「バージョン管理」が記載される。

【0070】

記述551において、「削除・破棄に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、及び、「完全消去」が記載される。

【0071】

記述561において、「参照に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「編集禁止のデータのみ参照許可」、「印刷禁止のデータのみ参照許可」、「参照場所限定のデータのみ参照許可」、及び、「ユーザ限定のデータのみ参照許可」が記載される。

【0072】

記述571において、「ネットワーク配信（送信）に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「信頼チャネルの利用（送信データの暗号化）」、「宛先制限（社内のみ配信可能など）」、「編集禁止のデータのみ配信許可」、「印刷禁止のみ配信許可」、「参照場所限定のデータのみ配信許可」、及び、「ユーザ限定のデータのみ配信許可」が記載される。

【0073】

記述581において、「ディスク配布（送付）に関わる要件」として、「明示的な許可

（利用制限）」、「監査証跡の記録」、「監査証跡のイメージ付き記録」、「送付データの暗号化」、「送付データの改ざん保護」、「編集禁止のデータのみ送付許可」、「印刷禁止のみ送付許可」、「参照場所限定のデータのみ送付許可」、及び、「ユーザ限定のデータのみ送付許可」が記載される。

【0074】

記述 5 9 1 において、「アーカイブ・バックアップに関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、「アーカイブデータの暗号化」、及び、「アーカイブデータの改ざん保護」が記載される。

【0075】

記述 6 0 1 において、「会議での利用に関わる要件」として、「明示的な許可（利用制限）」、「監査証跡の記録」、及び、「監査証跡のイメージ付き記録」が記載される。

【0076】

図 2 のドキュメントラベル用語ファイルと図 3 から図 1 3 のポリシー用語ファイルとに基づく DSP について図 1 4 から図 2 2 で説明する。図 1 4 から図 2 2 は、ポリシーファイルの例を示す図である。上述の図 2 に示すドキュメントラベル用語ファイル 3 0 0 と、図 3 から図 1 3 のポリシー用語ファイル 4 0 0 とに基づいて、ユーザの組織内でのセキュリティに対するポリシーが、例えば図 1 4 から図 2 2 に示す DSP 2 0 0 0 のように XML で記述され、1 つのポリシーファイルを構成する。

【0077】

図 1 4 から図 2 2 に示されるような DSP 2 0 0 0 は、<policy>で示される記述 2 0 0 1 から</policy>で示される記述 2 0 0 2 にてポリシーが示される。

【0078】

図 1 4 の<acc_rule>を示す記述 2 0 1 1 から図 1 6 の</acc_rule>を示す記述 2 0 1 2 において、<doc_category>ANY</doc_category>及び<doc_security_level>basic</doc_security_level>を示す記述 2 0 1 3 によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「basic（基本レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述 2 0 1 7 によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0079】

図 1 6 の<acc_rule>を示す記述 2 0 2 1 から図 1 9 の</acc_rule>を示す記述 2 0 2 2 において、<doc_category>ANY</doc_category>及び<doc_security_level>medium</doc_security_level>を示す記述 2 0 2 3 によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「medium（中レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述 2 0 2 7 によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリの種類）」（図 2 の記述 3 1 2、3 1 3 及び 3 1 4 参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0080】

また、同様のドキュメント属性を有するドキュメントに対して、図 1 8 の<user_category>ANY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述 2 0 2 8 によって、ユーザカテゴリ「ANY（非限定）」かつユーザセキュリティレベル

「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0081】

図19の<acc_rule>を示す記述2031から図19の</acc_rule>を示す記述2032において、<doc_category>ANY</doc_category>及び<doc_security_level>high</doc_security_level>を示す記述2023によって、ドキュメントカテゴリ「ANY（非限定）」かつドキュメントセキュリティレベル「high（高レベル）」であるドキュメント属性を有するドキュメントに対して、<user_category>DOC-CATEGORY</user_category>及び<user_security_level>ANY</user_security_level>を示す記述2037によって、ユーザカテゴリ「DOC-CATEGORY（文書カテゴリの種類）」（図2の記述312、313及び314参照）かつユーザセキュリティレベル「ANY（非限定）」であるユーザ属性を有するユーザが行うオペレーション毎のポリシーが記述される。<operation>から</operation>までの記述毎に、オペレーションの許可（<allowed/>）又は不許可（<denied/>）が規定される。更に、オペレーションが許可される場合は、許可するための要件（<requirement>）が規定される。

【0082】

次に、図14から図22のDSP2000の構造を、図23から図25を参照して、以下に、詳しく説明する。

【0083】

図23は、DSPの識別情報の例を示す図である。DSP2000の識別情報210において、<about_this_policy>と</about_this_policy>とで囲まれた範囲の記述211～213には、DSP2000を識別するための識別情報が記述される。

【0084】

<serial_number>RDSP2023</serial_number>を示す記述211には、DSP2000を他のDSPと区別するためのシリアル番号が記述される。

【0085】

<terminology_applied>RDST9487</terminology_applied>で示される記述212には、DSP2000に対応するポリシー用語ファイル400のシリアル番号が記述される。尚、この定義ファイルは更新される可能性があるため、このDSP2000がどのポリシー用語ファイルに基づいて記述されているのかを明確にするために記録しておく。記述213には、<title>DOCUMENT-SECURITY-POLICY</title>を示す記述によってDSP2000のタイトル、<version>1.20</version>を示す記述によってバージョン番号、<creation_date>2002/02/18 22:30:24</creation_date>を示す記述によって作成日時、<creator>Taro Tokyo</creator>を示す記述によって作成者、<description>sample document security policy.</description>を示す記述によって説明などの一般的な書誌情報が記述される。

【0086】

そして、DSP2000の識別情報は、</about_this_policy>により終了する。

【0087】

次に、上述のDSP2000の識別情報に続いて、ポリシーの内容を<policy>と</policy>で囲まれた範囲に記述する。図24は、DSPの構造を説明するための記述例を示す図である。

【0088】

図24に示されるポリシーの内容220は、以下に説明するように、階層構造を用いて記録する。

【0089】

ポリシー<policy>は、複数のアクセス制御ルール<acc_rule>（記述221）で構成される。一つのアクセス制御ルール<acc_rule>（記述221）は、対象とするドキュメントのカテゴリ<doc_category>とレベル<doc_security_level>を一意に指定し（記述222）

、さらにアクセス制御リスト<acl>（記述 2 2 3）を一つ含むように構成される。

【0090】

アクセス制御リスト<acl>（記述 2 2 3）は、複数のアクセス制御エレメント<ace>（記述 2 2 4）で構成される。

【0091】

各アクセス制御エレメント<ace>（記述 2 2 4）は、対象とするユーザのカテゴリ<user_category>（記述 2 2 5）とレベル<user_security_level>（記述 2 2 6）を一意に指定し、さらに複数のオペレーション<operation>（記述 2 2 7）で構成される。

【0092】

各<operation>（記述 2 2 7）は、一つのオペレーション名<name>（記述 2 2 8）と、一つの禁止<denied/>（記述 2 2 9）、または一つの許可<allowed/>（記述 2 3 2）、または複数の<requirement>（記述 2 3 0 及び記述 2 3 1）で構成される。

【0093】

記述 2 2 2 において、ドキュメントのカテゴリ<doc_category>やユーザのカテゴリ<user_category_level>に記述している” ANY” は、どのカテゴリ、及び、レベルにも適用されることを示している。また、記述 2 2 5 によって示されるユーザのカテゴリ<user_category>の” DOC-CATEGORY” は、ユーザのカテゴリがドキュメントのカテゴリと同じときに適用されることを示している。

【0094】

この実施例では、禁止するオペレーションには<denied/>（記述 2 2 9）を指定するようにしているが、DSP 2 0 0 0 に記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【0095】

このように、DSP を記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて、どのようなユーザタイプ（カテゴリ、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能の場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【0096】

そして、DSP を、上記のようにプラットフォームに依存しない XML で記述することにより、異なるタイプのシステム間で、この DSP を共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図 3 から図 1 3 のドキュメントラベルファイルや図 1 4 から図 2 2 の DSP 2 0 0 0 に記述しているように、紙ドキュメントに関するオペレーション（hardcopy, scan など）も規定できる。

【0097】

本実施例の、図 2 4 に示す要件の中に、以下の<requirement>explicit_authorization</requirement>を示す記述 2 3 1 が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、この DSP に従ってオペレーションがコントロールされるようになると、自由度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【0098】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと、明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【0099】

従って、DSP に記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、

ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまつてオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【0100】

次に本発明のDSPの別の記述形を図26で説明する。図25は、DSPの他の記述例を示す図である。図26に示すポリシーの内容240は、無条件で許可するオペレーションや、禁止するオペレーションが多くなった場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>を示す記述243と、許可しないオペレーションを列挙する、<denied_operations>を示す記述241を使用するようにしても良い。

【0101】

また、<requirement>explicit_authorization</requirement>を示す記述242は、図24での説明と同様である。

【0102】

図26は、上述のDSPを蓄積し且つ配布する種々の媒体を示す。

【0103】

以上で説明したように、図26に示されたDSP2000は、XML (Extensible Markup Language) で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク51、光磁気ディスク52、フレキシブルディスク53、又は、CD-ROM、CD-R、CD-RW、DVD、DVD-R、DVD-RAM、DVD-RW、DVD+RW、DVD+Rのような光ディスク54のような記憶媒体を作成することができる。また、その電子的なDSP2000をコンピュータ55を使用して、ネットワーク56を介してで伝送することができる。

【0104】

このDSP2000は、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従つて、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【0105】

図27は、本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。図27において、画像形成装置1000は、コンピュータによって制御される装置であつて、CPU (中央処理装置) 11と、ROM (Read-Only Memory) 12と、RAM (Random Access Memory) 13と、不揮発性RAM (non-volatile Random Access Memory) 14と、リアルタイムクロック15、イーサネット (登録商標) I/F (Ethernet (登録商標) Interface) 21と、USB (Universal Serial Bus) 22と、IEEE (Institute of Electrical and Electronics Engineers) 1284 23と、ハードディスク I/F 24と、エンジン I/F 25と、RS-232C I/F 26と、ドライバ27とで構成され、システムバスBに接続される。

【0106】

CPU 11は、ROM 12に格納されたプログラムに従つて画像形成装置1000を制御する。RAM 13には、例えば、各インターフェース21から26に接続される資源に領域が割り当てられる。不揮発性RAM 14には、画像形成装置1000を制御するためにCPU 11による処理に必要な情報が格納される。リアルタイムクロック15は、現時刻を計ると共に、処理を同期させる場合にCPU 11によって使用される。

【0107】

イーサネット (登録商標) I/F 21には、10BASE-T又は100BASE-TX等のイーサネット (登録商標) 用インターフェースケーブルが接続される。USB 22

には、USB用インターフェースケーブルが接続される。IEEE1284 23には、IEEE1284用インターフェースケーブルが接続される。

【0108】

ハードディスクI/F24には、ハードディスク34が接続され、ネットワークを介して送信された印刷すべき文書の文書データ、又は、印刷処理後の画像データがハードディスクI/F24を介してハードディスク34に格納される。エンジンI/F25には、文書データに基づいて所定媒体に印刷を行うプロッタ35-1及び画像データを取り込むスキャナ35-2等が接続される。RS-232C I/F26には、オペレーションパネル36が接続され、ユーザへの情報の表示及びユーザから入力情報又は設定情報の取得が行われる。

【0109】

画像形成装置1000によって行われる処理を実現するプログラムは、例えば、CD-ROM等の記憶媒体37によって画像形成装置1000に提供される。即ち、プログラムが保存された記憶媒体37がドライバ27にセットされると、ドライバ27が記憶媒体37からプログラムを読み出し、その読み出されたプログラムがシステムバスBを介してハードディスク34にインストールされる。そして、プログラムが起動されると、ハードディスク34にインストールされたプログラムに従ってCPU11がその処理を開始する。尚、プログラムを格納する記憶媒体37としてCD-ROMに限定するものではなく、コンピュータが読み取り可能な記憶媒体であればよい。プログラムをネットワークを介してダウンロードし、ハードディスク34にインストールするようにしても良い。

【0110】

セキュリティポリシーに従って動作する画像形成装置について図28、図29及び図30を参照して以下に詳細に説明する。

【0111】

図28は、セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。

【0112】

図28に示す読み取り装置としての画像形成装置1000は、主に、読み取り部71と、読み取り条件取得部72と、データ送信先取得部73と、データ処理部74と、データ送信部75と、ポリシー実行部1001と、読み取り画像データ61と、蓄積データ62とを有する。

【0113】

また、ポリシー実行部1001は、ドキュメント属性取得部1011と、動作要件選択部1012と、動作制御部1013と、ユーザ属性取得部1021とを有する。ドキュメント属性取得部1011は紙原稿60から又は読み取り画像データ61からドキュメント属性を取得して、動作要件選択部1012へ通知する。

【0114】

一方、ユーザ属性取得部1021は、ユーザによって入力されたユーザ情報を取得すると、動作要件選択部1012に通知する。動作要件選択部1012は、DSP2000に従って許可される場合の要件を選択し、その結果を動作制御部1013に通知する。動作制御部1013は、読み取った紙原稿60の画像データに対するデータ処理を指示する。

【0115】

ポリシー実行部1001において、点線で示される部分について省略しても良い。

【0116】

読み取り部71は、読み取り条件取得部72から通知されるユーザによって入力された読み取り条件に従って、紙原稿60を読み取る（スキャン）する処理部であり、読み取った画像データは、読み取り画像データ61に格納される。また、画像データ61から取得したドキュメント属性をドキュメント属性取得部1011に通知する。

【0117】

読み取り条件取得部72は、ユーザによって入力された読み取り条件を取得し、読み取

り部 71 とデータ処理部 74 とへ通知する。

【0118】

データ送信先取得部 73 は、ユーザによって入力されたデータ送信先を取得し、データ送信部 75 に通知する処理部である。

【0119】

データ処理部 74 は、動作制御部 1013 から提供される要件を満たすように読み取り条件取得部 72 から通知されるユーザによって入力された読み取り条件に従って、データ処理を読み取った画像データに行い、データ処理された画像データを蓄積データ 62 に蓄積する。

【0120】

データ送信部 75 は、動作制御部 1013 から通知される要件を満たすように、蓄積データ 62 から取り出した処理対象となる画像データをデータ送信先取得部 73 から通知された送信先へ送信する。

【0121】

画像データを外部に送信する必要がある場合、データ送信部 28 を省略しても良い。また、画像データを記憶媒体 37 に記憶するようにしても良い。

【0122】

図 28 において、読み取り装置としての画像形成装置 1000 は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。

【0123】

また、以下に説明する本発明の実施例をコンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記憶媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【0124】

図 29 は、簡略化した DSP の例を示す図である。説明の便宜のため、DSP 2000 を簡略化した DSP で説明する。図 29 に示される DSP 2100 において、つぎのようにルール 1 からルール 3 を示す。

【0125】

ルール 1 は、図 29 の第 4 行目の<acc_rule>から、第 10 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 11 行目<operation>から、第 14 行目</operation>までの部分により記述される。

【0126】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわらずルール 1 が適用されることを示す。

【0127】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルが basic のときを示す。

【0128】

第 9 行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわりないことを示す。

【0129】

第 10 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【0130】

更に第 12 行目と第 13 行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【0131】

従って、ルール 1 では、第 5 行目、第 6 行目、第 9 行目、第 10 行目、第 12 行目及び

第 1 3 行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが” basic” の場合には、ユーザのカテゴリーにかかわらず、且つ、ユーザのセキュリティレベルにかかわらず、読み取りは要件なく許可される。

【 0 1 3 2 】

次に、ルール 2 は、図 2 9 の第 4 行目の<acc_rule>から、第 1 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 1 5 行目<operation>から、第 2 0 行目</operation>までの部分により記述される。

【 0 1 3 3 】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわらずルール 2 が適用されることを示している。

【 0 1 3 4 】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【 0 1 3 5 】

第 9 行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわらないことを示す。

【 0 1 3 6 】

第 1 0 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらないことを示す。

【 0 1 3 7 】

更に、第 1 6 行目から第 1 9 行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【 0 1 3 8 】

従って、ルール 2 では、第 5 行目、第 6 行目、第 9 行目、第 1 0 行目、第 1 6 行目から第 1 9 行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが” basic” の場合には、ユーザのカテゴリーにかかわらず、且つ、ユーザのセキュリティレベルにかかわらず、ネットワーク配信は、ログを記録すること、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【 0 1 3 9 】

そして、ルール 3 は、図 2 9 の第 2 4 行目の<acc_rule>から、第 3 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 3 1 行目<operation>から、第 3 5 行目</operation>までの部分により記述される。

【 0 1 4 0 】

第 2 5 行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわらないことを示す。

【 0 1 4 1 】

第 2 6 行目の<doc_security_level>high</doc_security_level>は、文書のセキュリティレベルがhighの場合を示す。

【 0 1 4 2 】

第 2 9 行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【 0 1 4 3 】

第 3 0 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらないことを示す。

【0144】

第32行目から第34行目の、

<name>scan</name>

<requirement>audit</requirement>

<requirement>embed_trace_info</requirement>

は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【0145】

従って、ルール3では、第25行目、第26行目、第29行目、第30行目、第31行目から第34行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが”high”の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわらず、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【0146】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【0147】

図28を参照しつつ、詳細な動作について説明する。

【0148】

上述の図29に示すDSP2100に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【0149】

また、上述の図29に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【0150】

次に、セキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、動作制御部1013は、データ処理部71に対して、文書の読み取りを指示し、ユーザは文書データを取得して終了する。

【0151】

一方、セキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場合には、動作要件選択部1012は、その要件をすべて満たすことができるかを判定し、その判断結果を動作制御部1013に通知する。

【0152】

動作要件選択部1012による判断結果がすべての要件を満たすことができないことを示す場合は、動作制御部1013は、データ処理部74に対してデータ処理を禁止するように指示し、データ処理部74は読み取りデータを破棄して終了する。ユーザに対してはデータ処理が行えないことを通知する。

【0153】

一方、動作要件選択部1012による判断結果がすべての要件を満たすことができることを示す場合は、動作制御部1013データ処理部74に対して、その要件を満たすよう

にデータ処理を行うように指示する。ユーザは文書データを取得して終了する。

【0154】

この場合には、以下の処理が実行される。

【0155】

ユーザ属性取得部1021は、オペレーションパネル36から読み取り指示を出したユーザに、ユーザIDの入力要求を出す。ユーザは、オペレーションパネル36からユーザIDを入力する。ユーザ属性取得部1021は、ユーザIDからデータベース102に登録されている入力されたユーザIDに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部1021に通知する。

【0156】

ログを記録する場合、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【0157】

最後に、ユーザは紙原稿60の画像データを蓄積データ62内に取得して終了する。

【0158】

以上のように、図29に示したセキュリティポリシーに従って、紙原稿(ドキュメント)60を読み取ることができる。

【0159】

次に、画像形成装置1000が紙原稿60を読み取り且つ読み取った文書をネットワークに配信する場合について説明する。

【0160】

まず、ユーザが、画像形成装置1000に紙原稿60をセットし、オペレーションパネル36から、読み取り条件の入力、読み取りデータの配信先の指定及び紙原稿60の読み取り指示を出す。

【0161】

読み取り部71が、紙文書の読み取りを行う。ドキュメント属性取得部1011は、読み取った紙原稿60の画像データのバーコードや電子透かしなどの画像情報から文書IDを抽出し、カテゴリー、セキュリティレベルを取得して、動作要件選択部1012に通知する。

【0162】

動作要件選択部1012は、ドキュメント属性取得部1011が通知したドキュメント属性に従って、DSP2100の中に対応するエントリを検索し、要件を抽出する。

【0163】

上述の図29に示すDSP2100に基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【0164】

また、上述の図29に示すDSP2100に基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【0165】

例えば、ドキュメントをネットワークへ配信する際の要件が、DSP2100内に存在しない場合には、動作制御部1013は、データ送信部75に対して配信の指示を行い、

ドキュメントをネットワークへ配信して、処理を終了する。

【0166】

一方、例えば、ドキュメントをネットワークへ配信する際の要件が、DSP2100内に存在する場合には、動作要件選択部1012が、その要件をすべて満たすことができるかを判定する。

【0167】

ネットワークに配信することを許可するルールがない場合には、動作制御部1013が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、紙原稿60の画像データを破棄して終了する。例えば、セキュリティレベルが”high”の場合である。

【0168】

動作要件選択部1012によってすべての要件を満たすことができないと判断した場合は、動作制御部1013が、ユーザに通知をして、データ処理部74に対して紙原稿60の画像データを破棄するように指示して終了する。

【0169】

例えば、上述のセキュリティレベルが”basic”の場合のように、すべての要件を満たすことができる場合は、動作制御部1013は、その要件を満たした読み取りをデータ処理部74に指示し、また、データ送信部75にドキュメントをネットワークに配信するように指示して終了する。

【0170】

そして、ユーザ属性取得部1012は、オペレーションパネル36から読み取り指示を出したユーザに、ユーザIDの入力要求を出す。

【0171】

ユーザが、オペレーションパネル36からユーザIDを入力すると、ユーザ属性取得部1021は、ユーザIDに対応するカテゴリー、セキュリティレベルを取得し、動作要件選択部1012に通知する。動作制御部1013は、動作要件選択部1012から通知される要件に従ってログを記録する。

【0172】

更に、動作制御部1013は、データ処理部74に対して、読み取った紙原稿60の画像データを、印刷不可能なデータ(たとえばADOBE(登録商標)の印刷禁止属性を持ったPDFなど)に変換するように指示を行う。

【0173】

最後に、動作制御部1013は、データ送信部75に対して配信指示を行い、データ送信部75は、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、ドキュメントをネットワークへ配信し、終了する。

【0174】

以上のように、図29に示したDSP2100を使用して、図28に示した文書読み取り装置としての画像形成装置1000が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【0175】

セキュリティポリシーに従った動作を実現する複写装置としての画像形成装置の機能構成について図30で説明する。図30は、セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。図30中、図28と同様の処理部には同一符号を付しその詳細な説明を省略する。

【0176】

図30において、複写装置としての画像形成装置1000-2は、図28に示す画像形成装置1000の読み取り条件取得部72及びデータ送信先取得部73の代わりに複写条件取得部81と、図28に示す画像形成装置1000のデータ送信部75の代わりに印刷部82とを有する点において、図28に示す画像形成装置1000と異なっている。

【0177】

しかしながら、画像形成装置 1000 が画像形成装置 1000-2 の複写条件取得部 81 と、印刷部 82 とを更に有するように構成しても良い。点線で示される部分 1002 は省略しても良い。

【0178】

複写条件取得部 81 は、ユーザがオペレーションパネル 36 に入力した複写条件を取得して、読み取り部 71 とデータ処理部 74 とへ複写条件を通知すると共に、印刷部 82 へも通知する。

【0179】

印刷部 82 は、動作制御部 1013 からの指示に応じて、蓄積データ 62 から紙原稿 60 の画像データを取得し、動作制御部 1013 から通知された要件を満たすように複写条件取得部 81 から通知された複写条件に従って印刷処理を行い、用紙に画像データが形成された複写原稿 60b を出力する。

【0180】

以下に、ドキュメント属性取得部 1011 とユーザ属性取得部 1021 について詳述する。

【0181】

図 31 は、ドキュメントの識別情報をバーコードで印字した場合を示す図である。図 31 に示すドキュメント 610 では、所定位置にバーコード 611 で識別情報が印字されている。この場合、ドキュメント属性取得部 1011 は、図 32 に示すように、紙原稿 60 としてのドキュメント 610 から直接識別情報を取得し、その識別情報からドキュメント属性を取得するように構成される。

【0182】

図 32 は、ドキュメント属性取得部の第一機能構成を示す図である。図 32 において、ドキュメント属性取得部 1011-1 は、識別情報取得部 1031 と、ドキュメント属性読み取り部 1032 と、ドキュメント属性 DB 64 とを有する。

【0183】

識別情報取得部 1031 は、紙原稿 60 から図 31 に示されるドキュメント 610 のバーコード 611 を読み取って、識別情報として取得し、ドキュメント属性読み取り部 1032 に通知する。

【0184】

ドキュメント属性読み取り部 1032 は、テーブル T100 を参照することによって、識別情報取得部 1031 から通知された識別情報に基づいてドキュメント属性を取得して、動作要件選択部 1012 へ通知する。

【0185】

ドキュメント属性 DB 1011-1 は、テーブル T100 によってドキュメント属性を管理する。テーブル T100 は、識別情報としてドキュメント ID、カテゴリー、レベル、取り扱い可能ゾーン等の項目を有する。ドキュメント属性読み取り部 1032 は、ドキュメント属性として、カテゴリー、レベル、取り扱い可能ゾーン等の情報を取得することができる。

【0186】

このような機能構成は、バーコード、RFID、MCR 等の専用の読み取り装置が既に利用されている場合に適している。

【0187】

図 33 は、ドキュメントの識別情報を数字で印字した場合を示す図である。図 33 に示すドキュメント 620 では、所定位置に数字 621 で識別情報が印字されている。この場合、ドキュメント属性取得部 1011 は、図 34 に示すように、紙原稿 60 としてのドキュメント 610 から直接識別情報を取得し、その識別情報からドキュメント属性を取得するように構成される。

【0188】

図 34 は、ドキュメント属性取得部の第二機能構成を示す図である。図 34 中、図 32

と同様の処理部には同一の符号を付し、その説明を省略する。

【0189】

図34において、ドキュメント属性取得部1011-2は、識別情報取得部1031と、ドキュメント属性読み取り部1032と、ドキュメント属性DB64とを有する点で図32に示すドキュメント属性取得部1011-1と同様であるが、一旦読み取り部71によって読み取った紙原稿60の画像データが格納されている読み取り画像データ61からその画像データを取り出して、OCR等の文字認識機能を利用して識別することによって、ドキュメント属性を取得する点が異なっている。テーブルT100のデータ構成も図32に示すドキュメント属性取得部1011-1と同様である。

【0190】

図35は、ドキュメントの識別情報を前面に印字した場合を示す図である。図35に示すドキュメント630では、前面に識別情報を示すドットパターンが印字されている。

【0191】

図36は、ドキュメントのセキュリティ属性を文字で印字した場合を示す図である。図36に示すドキュメント640は、所定位置に例えばドキュメント属性を示す「秘」641が直接印字されている。

【0192】

このような場合、読み取り部71によって取得した画像データをOCRなどで文字認識し、所定位置に印字されているドキュメント属性を取得する。

【0193】

図37は、ドキュメント属性取得部の第三機能構成を示す図である。図37において、ドキュメント属性取得部1011-3は、文字読み取り部1035と、カテゴリ辞書65と、レベル辞書66と、取り扱いゾーン辞書67等を夫々管理するデータベースとを有する。

【0194】

次に、ユーザ属性取得部1021について詳述する。

【0195】

図38は、ユーザ属性取得部の機能構成を示す図である。図38において、ユーザ属性取得部1021は、ユーザ情報取得部1041と、ユーザ認証部1042と、ユーザ属性読み取り部1043と、ユーザ属性DB68とを有する。

【0196】

ユーザ情報取得部1041は、ユーザによってオペレーションパネル36に入力されたユーザ情報を取得して、ユーザ認証部1042に通知する。

【0197】

ユーザ認証部1042は、ユーザ属性DB68を参照することによって、ユーザ情報に基づいて、ユーザ認証を行い、認証が成功した場合にユーザ属性を取得して、ユーザ属性読み取り部1043に通知する。

【0198】

ユーザ属性DB68は、ユーザ情報としてユーザIDとパスワードの項目を有し、ユーザ属性としてカテゴリ、レベル等の項目を有するテーブルT200によってユーザ属性を管理する。

【0199】

ユーザ属性読み取り部1043は、ユーザ属性を動作要件選択部1012に通知する。

【0200】

ドキュメント属性と同様に外部サーバによって実現することも可能である。外部サーバを利用することで、Windows（登録商標）、Lotus Notesなどを利用するユーザ等との連携が容易に実現可能となる。

【0201】

図39は、ユーザ属性を外部サーバから取得する場合の機能構成を示す図である。図39中、図38と同様の処理部には同一の符号を付し、その説明を省略する。図39

において、ユーザ属性取得部 1 0 1 2 - 2 は、ユーザ情報取得部 1 0 4 1 と通信処理部 1 0 4 5 とを有する。

【0 2 0 2】

通信処理部 1 0 4 5 は、外部サーバとしてのユーザ属性サーバ 8 0 へ、ユーザ情報を送信することによってユーザ属性の要求を行い、ユーザ属性サーバ 8 0 から取得したユーザ属性を動作要件選択部 1 0 1 2 に通知する。

【0 2 0 3】

外部サーバとしてのユーザ属性サーバ 8 0 は、通信処理部 8 5 と、ユーザ認証部 8 2 と、ユーザ属性読み取り部 8 3 と、ユーザ属性 DB 6 9 とを有する。

【0 2 0 4】

通信処理部 8 5 は、ユーザ属性取得部 1 0 2 1 - 2 からの要求に応じて、ユーザ情報をユーザ認証部 8 2 に通知する。

【0 2 0 5】

ユーザ認証部 8 2 は、ユーザ属性 DB 6 8 9 参照することによって、ユーザ情報に基づいて、ユーザ認証を行い、認証が成功した場合にユーザ属性を取得して、通信処理部 8 5 に通知する。

【0 2 0 6】

通信処理部 8 5 は、ユーザ属性をユーザ属性取得部 1 0 2 1 - 2 に通知する。

【0 2 0 7】

上述より、埋め込み情報が文書を一意に識別するバーコード情報、透かし情報、地紋情報のうち少なくとも一つの情報であることにより、埋め込み情報で文書のコンテンツや文書属性を識別して文書に関する処理が実行されるため、文書のセキュリティを確保することができる。

【0 2 0 8】

本発明の一実施例に係る画像形成装置 1 0 0 0 は、プリンタ、FAX、コピー等の複数の異なる画像形成機能の少なくとも 1 つを有する装置である。

【図面の簡単な説明】

【0 2 0 9】

【図 1】 セキュリティポリシーの例を示す図である。

【図 2】 ドキュメントラベル用語ファイルのリストの例を示す図である。

【図 3】 ポリシー用語ファイルの例を示す図である。

【図 4】 ポリシー用語ファイルの例を示す図である。

【図 5】 ポリシー用語ファイルの例を示す図である。

【図 6】 ポリシー用語ファイルの例を示す図である。

【図 7】 ポリシー用語ファイルの例を示す図である。

【図 8】 ポリシー用語ファイルの例を示す図である。

【図 9】 ポリシー用語ファイルの例を示す図である。

【図 1 0】 ポリシー用語ファイルの例を示す図である。

【図 1 1】 ポリシー用語ファイルの例を示す図である。

【図 1 2】 ポリシー用語ファイルの例を示す図である。

【図 1 3】 ポリシー用語ファイルの例を示す図である。

【図 1 4】 ポリシーファイルの例を示す図である。

【図 1 5】 ポリシーファイルの例を示す図である。

【図 1 6】 ポリシーファイルの例を示す図である。

【図 1 7】 ポリシーファイルの例を示す図である。

【図 1 8】 ポリシーファイルの例を示す図である。

【図 1 9】 ポリシーファイルの例を示す図である。

【図 2 0】 ポリシーファイルの例を示す図である。

【図 2 1】 ポリシーファイルの例を示す図である。

【図 2 2】 ポリシーファイルの例を示す図である。

【図 23】DSP の識別情報の例を示す図である。

【図 24】DSP の構造を説明するための記述例を示す図である。

【図 25】DSP の他の記述例を示す図である。

【図 26】DSP を蓄積し且つ配布する種々の媒体を示す図である。

【図 27】本発明の一実施例に係る画像形成装置のハードウェア構成を示すブロック図である。

【図 28】セキュリティポリシーに従って動作する読み取り装置としての画像形成装置の機能構成を示す図である。

【図 29】簡略化した DSP の例を示す図である。

【図 30】セキュリティポリシーに従って動作する複写装置としての画像形成装置の機能構成を示す図である。

【図 31】ドキュメントの識別情報をバーコードで印字した場合を示す図である。

【図 32】ドキュメント属性取得部の第一機能構成を示す図である。

【図 33】ドキュメントの識別情報を数字で印字した場合を示す図である。

【図 34】ドキュメント属性取得部の第二機能構成を示す図である。

【図 35】ドキュメントの識別情報を前面に印字した場合を示す図である。

【図 36】ドキュメントのセキュリティ属性を文字で印字した場合を示す図である。

【図 37】ドキュメント属性取得部の第三機能構成を示す図である。

【図 38】ユーザ属性取得部の機能構成を示す図である。

【図 39】ユーザ属性を外部を外部サーバから取得する場合の機能構成を示す図である。

【符号の説明】

【0210】

51	ハードディスク
52	光磁気ディスク
53	フレキシブルディスク
54	光ディスク
55	コンピュータ
56	ネットワーク
71	読み取り部
72	読み取り条件取得部
73	データ送信先取得部
74	データ処理部
1000	画像形成装置
1001	ポリシー実行部
1011	ドキュメント属性取得部
1012	動作要件選択部
1013	動作制御部
1021	ユーザ属性取得部
2000	DSP

【書類名】 図面
【図 1】

ドキュメントに関するセキュリティポリシーの例を示す図

201

202 極秘文書について:

原則複写禁止（複写する際には管理責任者の許可を得なければならない）、
また、複写したことを記録しておかなければならない
プリントする際には複写禁止であることを示す透かしを入れなければならない
ない、また、プリントしたことを記録しておかなければならない
閲覧は関係者のみ許可

203 丸秘文書について:

複写は関係者のみ許可
プリントする際には丸秘文書であることを示すラベルを同時に印刷しな
ければならない
閲覧は関係者のみ許可

204 社外秘文書について:

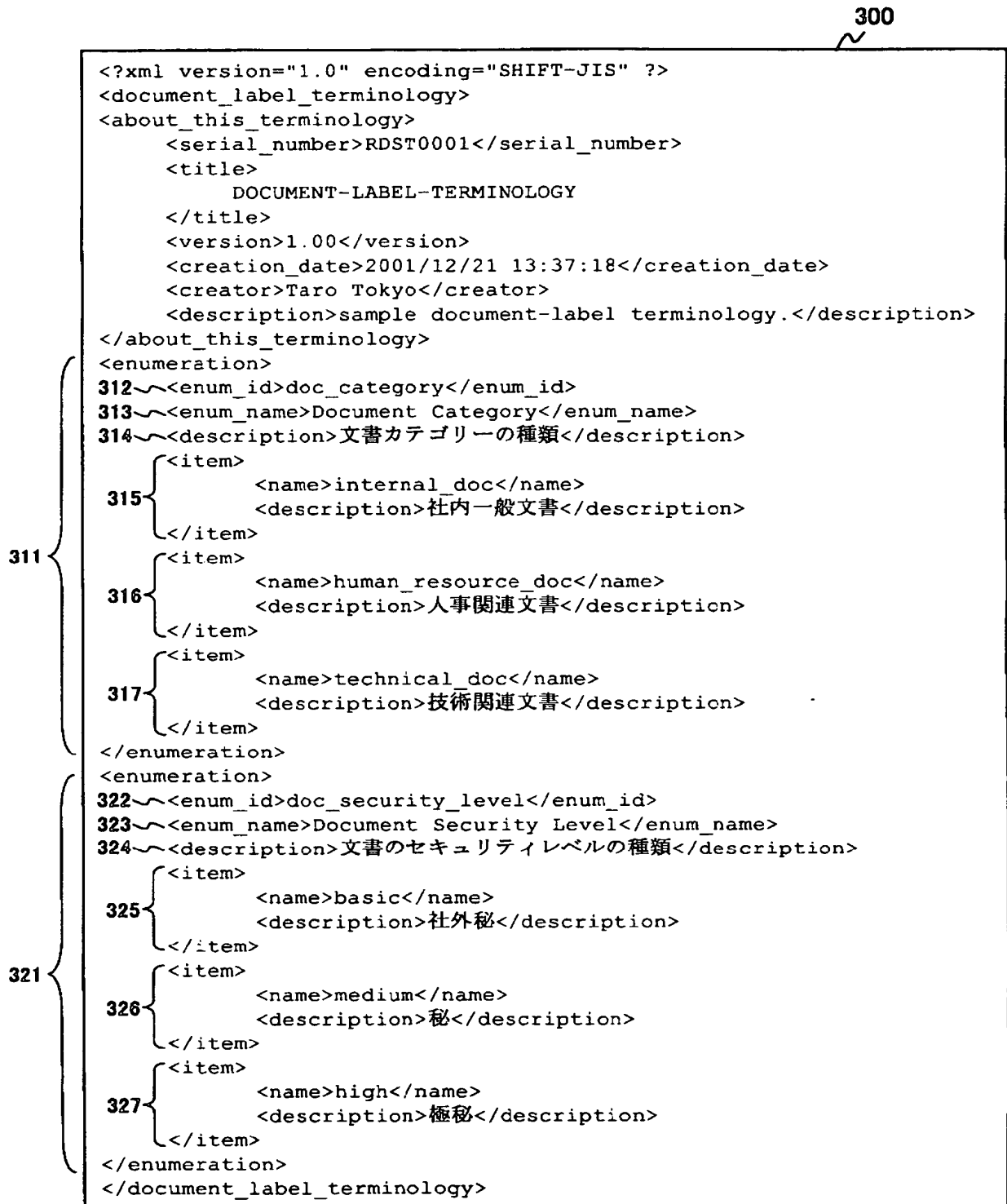
社外へ送付する際には管理責任者の許可を得なければならない
複写 プリント 閲覧は社内であれば許可不要

205 人事関連文書について:

すべて丸秘文書として取り扱う

【図2】

ドキュメントラベルファイルの例を示す図



【図 3】

ポリシー用語ファイルの例を示す図

400

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
  <about_this_terminology>
    <serial_number>RDST9487</serial_number>
    <title>DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
    <version>1.00</version>
    <creation_date>2001/12/21 13:37:18</creation_date>
    <creator>Taro Tokyo</creator>
    <description>sample policy terminology.</description>
  </about_this_terminology>

  <!-- システムタイプの列挙 -->
  <enumeration>
    <enum_id>system_type</enum_id>
    <enum_name>System Type</enum_name>
    <description>システムタイプの種類</description>
    <item>
      <name>Copier</name>
      <description>複写機</description>
      <operation>copier_operation</operation>
    </item>
    <item>
      <name>Printer</name>
      <description>プリンタ</description>
      <operation>printer_operation</operation>
    </item>
    <item>
      <name>Facsimile</name>
      <description>ファクシミリ</description>
      <operation>fax_operation</operation>
    </item>
    <item>
      <name>Scanner</name>
      <description>スキャナ</description>
      <operation>scanner_operation</operation>
    </item>
    <item>
      <name>Document Repository</name>
      <description>文書リポジトリ</description>
      <operation>repository_operation</operation>
    </item>
    <item>
      <name>E-Meeting</name>
      <description>電子会議システム</description>
      <operation>emeeting_operation</operation>
    </item>
  </enumeration>
```

411

【図 4】

ポリシー用語ファイルの例を示す図

```
400 ~
<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
  <enum_id>copier_operation</enum_id>
  <enum_name>Copier Operation</enum_name>
  <description>複写機に関わるオペレーション</description>
  <item>
    <name>hardcopy</name>
    <description>紙から紙への複写</description>
    <requirement>hardcopy_requirement</requirement>
  </item>
</enumeration>
421 {
  <enumeration>
    <enum_id>printer_operation</enum_id>
    <enum_name>Printer Operation</enum_name>
    <description>プリンタに関わるオペレーション</description>
    <item>
      <name>print</name>
      <description>電子文書を紙へ印刷</description>
      <requirement>print_requirement</requirement>
    </item>
  </enumeration>
431 {
  <enumeration>
    <enum_id>fax_operation</enum_id>
    <enum_name>Facsimile Operation</enum_name>
    <description>ファックスに関わるオペレーション</description>
    <item>
      <name>fax_send</name>
      <description>ファックスの送信</description>
      <requirement>fax_send_requirement</requirement>
    </item>
    <item>
      <name>fax_receive</name>
      <description>ファックスの受信</description>
      <requirement>fax_receive_requirement</requirement>
    </item>
  </enumeration>
441 {
  <enumeration>
    <enum_id>scanner_operation</enum_id>
    <enum_name>Scanner Operation</enum_name>
    <description>スキャナに関わるオペレーション</description>
    <item>
      <name>scan</name>
      <description>紙文書をスキャンして電子文書にする</description>
      <requirement>scan_requirement</requirement>
    </item>
  </enumeration>
451 {
  </enumeration>
~
```

【図 5】

ポリシー用語ファイルの例を示す図

```
400 ~
<enumeration>
  <enum_id>repository_operation</enum_id>
  <enum_name>Document Repository Operation</enum_name>
  <description>文書リポジトリに関わるオペレーション</description>
  <item>
    <name>store</name>
    <description>保存する</description>
    <requirement>store_requirement</requirement>
  </item>
  <item>
    <name>revise</name>
    <description>改訂・編集する</description>
    <requirement>revise_requirement</requirement>
  </item>
  <item>
    <name>delete</name>
    <description>削除・破棄する</description>
    <requirement>delete_requirement</requirement>
  </item>
  <item>
    <name>read</name>
    <description>参照する</description>
    <requirement>read_requirement</requirement>
  </item>
  <item>
    <name>net_delivery</name>
    <description>
      ネットワークで配布する（送信する）
    </description>
    <requirement>net_delivery_requirement</requirement>
  </item>
  <item>
    <name>disc_delivery</name>
    <description>ディスクで配布する（送付する）</description>
    <requirement>disc_delivery_requirement</requirement>
  </item>
  <item>
    <name>archive</name>
    <description>アーカイブ・バックアップする</description>
    <requirement>archive_requirement</requirement>
  </item>
</enumeration>
461 ~
<enumeration>
  <enum_id>emeeting_operation</enum_id>
  <enum_name>E-Meeting Operation</enum_name>
  <description>電子会議システムに関わるオペレーション</description>
  <item>
    <name>meeting_use</name>
    <description>会議で利用する</description>
    <requirement>meeting_use_requirement</requirement>
  </item>
</enumeration>
471 ~
```

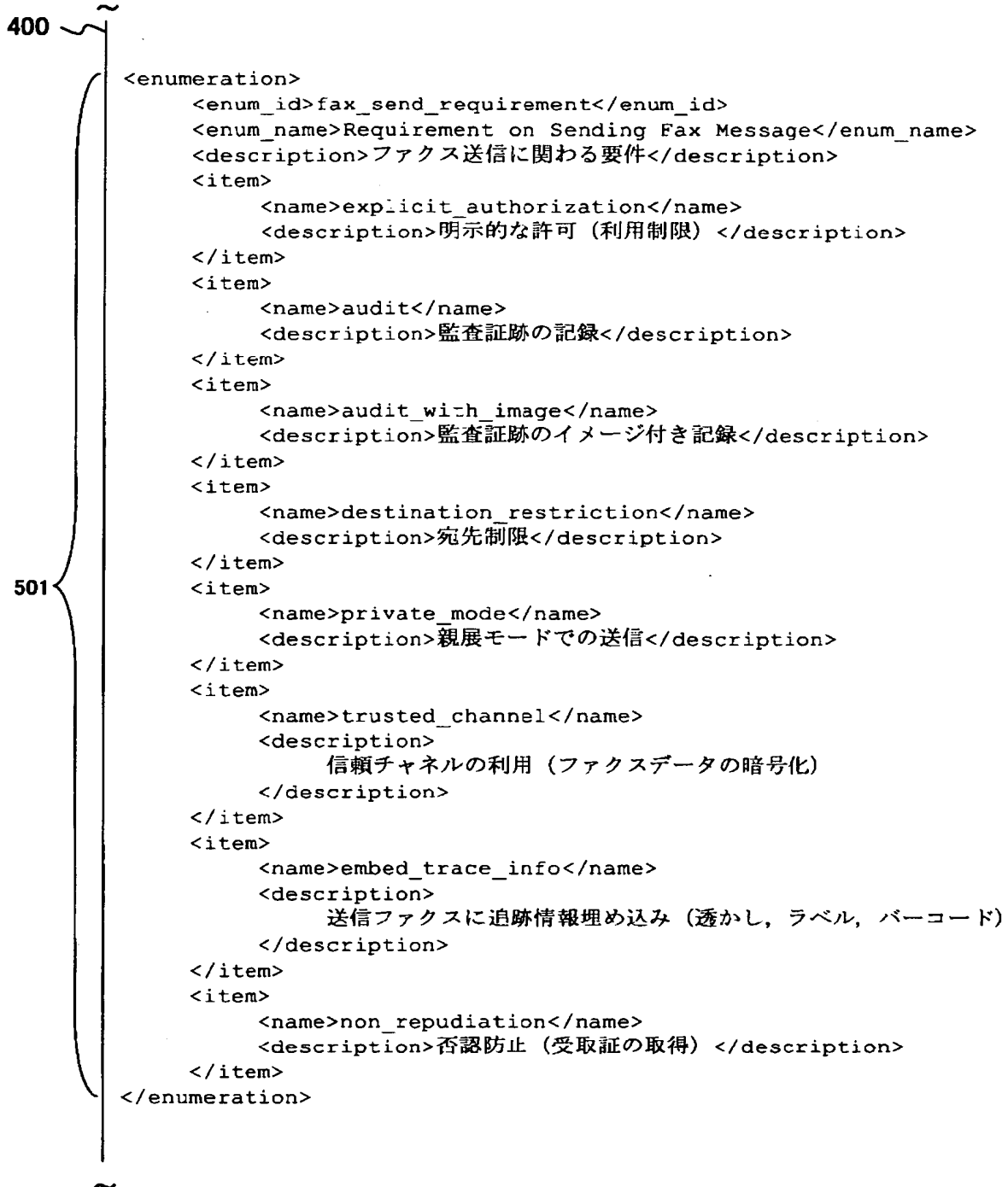
【図 6】

ポリシー用語ファイルの例を示す図

```
400 ~
<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証, 文書識別, アクセス制御 (利用制限) は基本メカニズムとして提供されるため
, 要件には含めない -->
<enumeration>
  <enum_id>hardcopy_requirement</enum_id>
  <enum_name>Hardcopy Requirement</enum_name>
  <description>複写に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可</description>
  </item>
481 <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
</enumeration>
<enumeration>
  <enum_id>print_requirement</enum_id>
  <enum_name>Print Requirement</enum_name>
  <description>印刷に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
491 <item>
    <name>private_access</name>
    <description>プリントした本人による紙出力</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>
      信頼チャネルの利用 (印刷データの暗号化)
    </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>
      プリントアウトに追跡情報埋め込み (透かし, ラベル, バーコード)
    </description>
  </item>
</enumeration>
~
```


【図 7】

ポリシー用語ファイルの例を示す図



【図 8】

ポリシー用語ファイルの例を示す図

```
400 ~
{
  <enumeration>
    <enum_id>fax_receive_requirement</enum_id>
    <enum_name>Requirement on Receiving Fax Message</enum_name>
    <description>ファックス受信に関わる要件</description>
    <item>
      <name>audit</name>
      <description>監査証拠の記録</description>
    </item>
    <item>
      <name>audit_with_image</name>
      <description>監査証拠のイメージ付き記録</description>
    </item>
    <item>
      <name>private_access</name>
      <description>親展ファックスの宛先本人による取り出し</description>
    </item>
    <item>
      <name>trusted_timestamp</name>
      <description>信頼タイムスタンプ</description>
    </item>
    <item>
      <name>embed_trace_info</name>
      <description>
        受信ファックスに追跡情報埋め込み (透かし, ラベル, バーコード)
      </description>
    </item>
  </enumeration>
  <enumeration>
    <enum_id>scan_requirement</enum_id>
    <enum_name>Scan Requirement</enum_name>
    <description>スキャンに関わる要件 (保存した後については保存要件を適用する)</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可 (利用制限) </description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証拠の記録</description>
    </item>
    <item>
      <name>audit_with_image</name>
      <description>監査証拠のイメージ付き記録</description>
    </item>
    <item>
      <name>embed_trace_info</name>
      <description>
        スキャン画像に追跡情報埋め込み (透かし, ラベル, バーコード)
      </description>
    </item>
  </enumeration>
}
521 ~
```

【図 9】

ポリシー用語ファイルの例を示す図

```
400 ~
<enumeration>
  <enum_id>store_requirement</enum_id>
  <enum_name>Store Requirement</enum_name>
  <description>保存に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>encryption</name>
    <description>保存データの暗号化</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>保存データの改ざん保護</description>
  </item>
</enumeration>
531 ~
<enumeration>
  <enum_id>revise_requirement</enum_id>
  <enum_name>Revise Requirement</enum_name>
  <description>改訂に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>versioning</name>
    <description>バージョン管理</description>
  </item>
</enumeration>
541 ~
```

【図10】

ポリシー用語ファイルの例を示す図

```
400 ~
<enumeration>
  <enum_id>delete_requirement</enum_id>
  <enum_name>Delete Requirement</enum_name>
  <description>削除・破棄に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>complete_erase</name>
    <description>完全消去</description>
  </item>
</enumeration>
551 ~
<enumeration>
  <enum_id>read_requirement</enum_id>
  <enum_name>Read Requirement</enum_name>
  <description>参照に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ参照許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ参照許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ参照許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ参照許可</description>
  </item>
</enumeration>
561 ~
```

【図 11】

ポリシー用語ファイルの例を示す図

400 ~

```
<enumeration>
  <enum_id>net_delivery_requirement</enum_id>
  <enum_name>Delivery via Network Requirement</enum_name>
  <description>ネットワーク配信（送信）に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証拠のイメージ付き記録</description>
  </item>
  <item>
    <name>trusted_channel</name>
    <description>信頼チャネルの利用（送信データの暗号化）
</description>
  </item>
  <item>
    <name>destination_restriction</name>
    <description>宛先制限（社内のみ配信可能など）</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ配信許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ配信許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ配信許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ配信許可</description>
  </item>
</enumeration>
```

571 ~

【図 12】

ポリシー用語ファイルの例を示す図

400 ~

```
<enumeration>
  <enum_id>disc_delivery_requirement</enum_id>
  <enum_name>Delivery via Disc Requirement</enum_name>
  <description>ディスク配布（送付）に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可（利用制限）</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録</description>
  </item>
  <item>
    <name>encryption</name>
    <description>送付データの暗号化</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>送付データの改ざん保護</description>
  </item>
  <item>
    <name>edit_restriction</name>
    <description>編集禁止のデータのみ送付許可</description>
  </item>
  <item>
    <name>print_restriction</name>
    <description>印刷禁止のデータのみ送付許可</description>
  </item>
  <item>
    <name>location_restriction</name>
    <description>参照場所限定のデータのみ送付許可</description>
  </item>
  <item>
    <name>user_restriction</name>
    <description>ユーザ限定のデータのみ送付許可</description>
  </item>
</enumeration>
```

581 ~

【図 13】

ポリシー用語ファイルの例を示す図

```
400 ~
{
  <enumeration>
    <enum_id>archive_requirement</enum_id>
    <enum_name>Archive Requirement</enum_name>
    <description>アーカイブ・バックアップに関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可（利用制限）</description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>encryption</name>
      <description>アーカイブデータの暗号化</description>
    </item>
    <item>
      <name>integrity_protection</name>
      <description>アーカイブデータの改ざん保護</description>
    </item>
  </enumeration>
  <enumeration>
    <enum_id>meeting_use_requirement</enum_id>
    <enum_name>Meeting-use Requirement</enum_name>
    <description>会議での利用に関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可（利用制限）</description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>audit_with_image</name>
      <description>監査証跡のイメージ付き記録</description>
    </item>
  </enumeration>
</policy_terminology>
591 ~
601 ~
```

【図 14】

ポリシーファイルの例を示す図

```

2000 <?xml version="1.0" encoding="SHIFT-JIS" ?>
      <document_security_policy>
        <about_this_policy>
          <serial_number>RDSP2023</serial_number>
          <terminology_applied>RDST9487</terminology_applied>
          <title>DOCUMENT-SECURITY-POLICY</title>
          <version>1.30</version>
          <creation_date>2002/02/18 22:30:24</creation_date>
          <creator>Taro Tokyo</creator>
          <description>sample document security policy.</description>
        </about_this_policy>
2001 <policy>
      <acc_rule>~ 2011
2013 { <doc_category>ANY</doc_category>
      { <doc_security_level>basic</doc_security_level>
      <acl>
        <ace>
2017 { <user_category>ANY</user_category>
      { <user_security_level>ANY</user_security_level>
        <operation>
          <name>hardcopy</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>print</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>fax_send</name>
          <requirement>audit</requirement>
          <requirement>explicit_authorization</requirement>
        </operation>
        <operation>
          <name>fax_receive</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
      }
    }
  }

```




【図 15】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>store</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
</acl>
</acc_rule> 2012
```

【図 16】

ポリシーファイルの例を示す図

2000

```

<acc_rule>~2021
2023 { <doc_category>ANY</doc_category>
      <doc_security_level>medium</doc_security_level>
      <acl>
        <ace>
          2027 { <user_category>DOC-CATEGORY</user_category>
                <user_security_level>ANY</user_security_level>
                <operation>
                  <name>hardcopy</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>print</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>fax_send</name>
                  <denied/>
                  <!-- denied even if it is explicitly authorized -->
                </operation>
                <operation>
                  <name>fax_receive</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
                <operation>
                  <name>scan</name>
                  <requirement>audit</requirement>
                  <requirement>embed_trace_info</requirement>
                </operation>
                <operation>
                  <name>store</name>
                  <allowed/><!-- allowed without any requirement -->
                </operation>
              }
        }
      }
    }
  }

```

【図 17】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>revise</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>delete</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
  <requirement>trusted_channel</requirement>
</operation>
<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>meeting_use</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
</ace>
```

【図 18】

ポリシーファイルの例を示す図

2000

```
<ace>
2028 {<user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>store</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>revise</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>delete</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }
```



【図 19】

ポリシーファイルの例を示す図

2000

```

<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
</ace>
</acl>
</acc_rule>
<acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    <ace>
      <user_category>DOC-CATEGORY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <requirement>explicit_authorization</requirement>
        <requirement>audit</requirement>
        <requirement>private_access</requirement>
        <requirement>trusted_channel</requirement>
        <requirement>embed_trace_info</requirement>
      </operation>
    </ace>
  </acl>
</acc_rule>

```

【図 20】

ポリシーファイルの例を示す図

2000

```
<operation>
  <name>fax_send</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>fax_receive</name>
  <allowed/><!-- allowed without any requirement -->
</operation>
<operation>
  <name>scan</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>store</name>
  <requirement>audit</requirement>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>revise</name>
  <requirement>versioning</requirement>
</operation>
<operation>
  <name>delete</name>
  <requirement>complete_erase</requirement>
</operation>
<operation>
  <name>read</name>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
```

【図 21】

ポリシーファイルの例を示す図

2000

```

<operation>
  <name>disc_delivery</name>
  <requirement>audit</requirement>
  <requirement>explicit_authorization</requirement>
  <requirement>encryption</requirement>
  <requirement>print_restriction</requirement>
</operation>
<operation>
  <name>archive</name>
  <requirement>encryption</requirement>
  <requirement>integrity_protection</requirement>
</operation>
<operation>
  <name>meeting_use</name>
  <requirement>explicit_authorization</requirement>
</operation>
</ace>
<ace>
2038 { <user_category>ANY</user_category>
      <user_security_level>ANY</user_security_level>
      <operation>
        <name>hardcopy</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>print</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_send</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>fax_receive</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
      <operation>
        <name>scan</name>
        <denied/>
        <!-- denied even if it is explicitly authorized -->
      </operation>
    }

```

【図 22】

ポリシーファイルの例を示す図

2000

```

<operation>
  <name>store</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>revise</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>delete</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>read</name>
  <requirement>explicit_authorization</requirement>
  <requirement>audit</requirement>
  <requirement>print_restriction</requirement>
  <requirement>location_restriction</requirement>
  <requirement>user_restriction</requirement>
</operation>
<operation>
  <name>net_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>disc_delivery</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>archive</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
<operation>
  <name>meeting_use</name>
  <denied/>
  <!-- denied even if it is explicitly authorized -->
</operation>
</ace>
</acl>
</acc_rule>

```

2002

2032

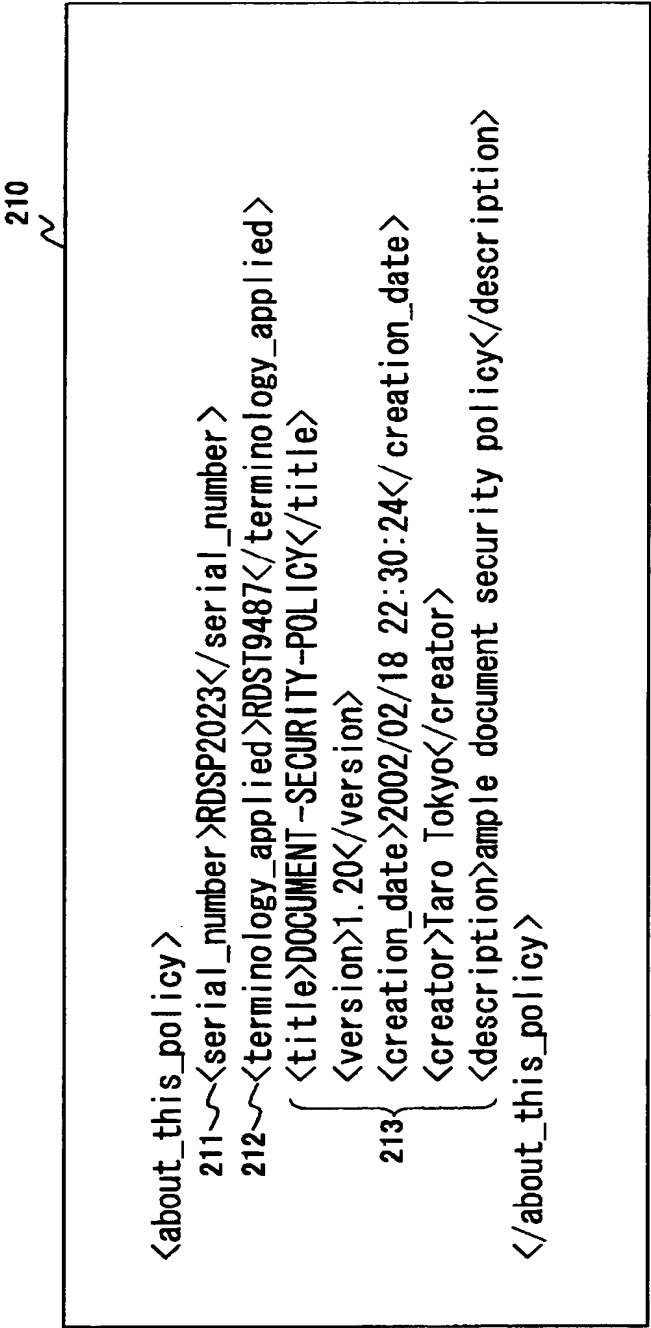
```

</policy>
</document_security_policy>

```


【図 2 3】

DSPの識別情報を示す図



【図 24】

DSPの構造を説明するための記述例を示す図

220
~

```

<policy>
221 ~ <acc_rule>
    232 { <doc_category>ANY</doc_category>
        <doc_security_level>medium</doc_security_level>
    223 ~ <acl>
        224 ~ <ace>
            225 ~ <user_category>DOC-CATEGORY
                </user_category>
            226 ~ <user_security_level>ANY
                </user_security_level>
            227 ~ <operation>
                228 ~ <name>fax_send</name>
                229 ~ <denied/><!-- denied even if it
                    is explicitly authorized -->
            </operation>
            227 ~ <operation>
                <name>net_delivery</name>
                230 ~ <requirement>audit
                    </requirement>
                231 ~ <requirement>
                    explicit_authorization
                </requirement>
                ...
            </operation>
            227 ~ <operation>
                <name>fax_receive</name>
                232 ~ <allowed/><!--allowed
                    without requirements -->
            </operation>
            ...
        </ace>
        <ace>
            ...
        </ace>
    </acl>
</acc_rule>
221 ~ <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
        ...
    </acl>
</acc_rule>
</policy>

```

【図 25】

DSPの他の記述例を示す図

240

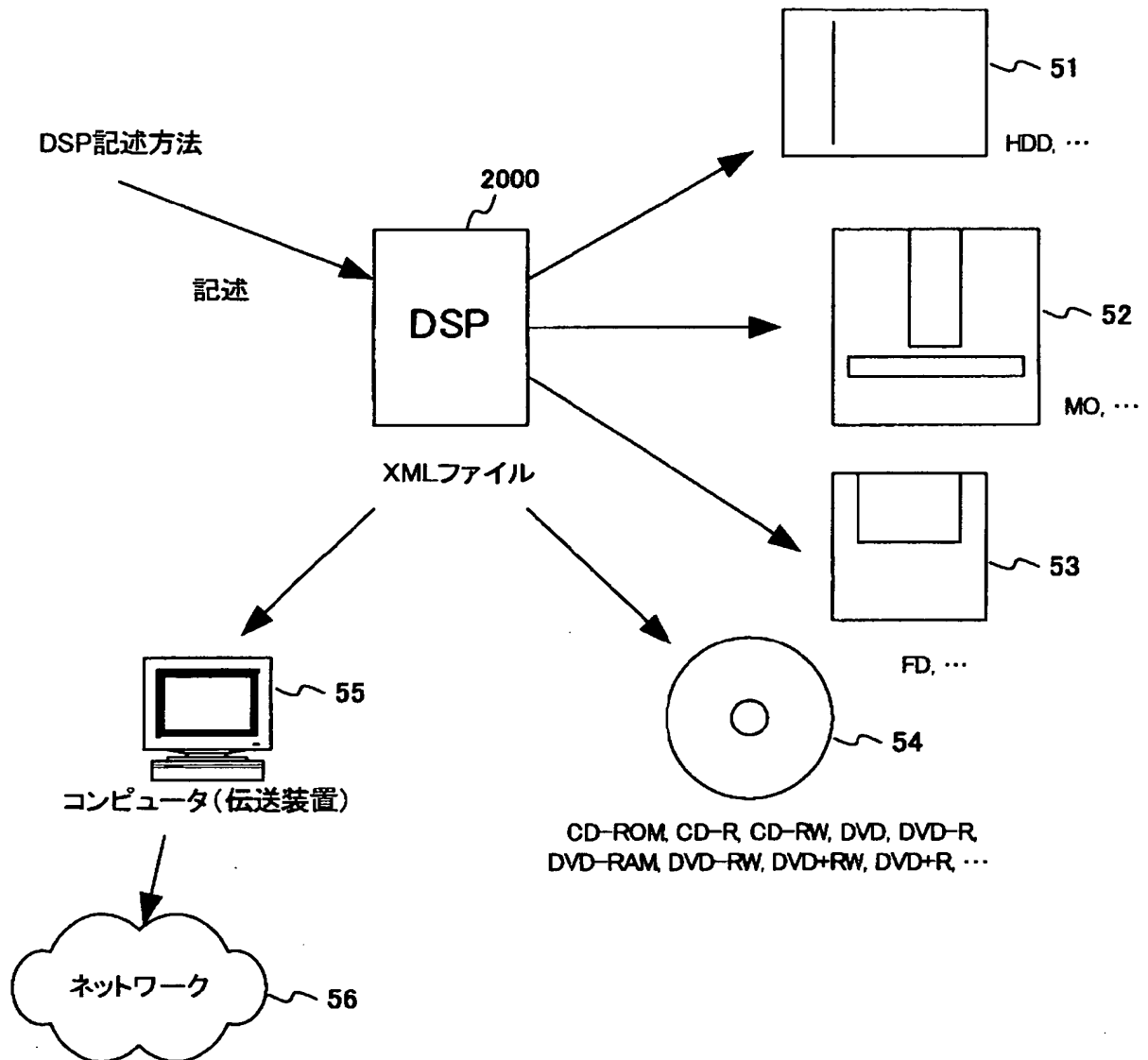
```

<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        241 ~ <denied_operations>
          <!-- denied even if it is explicitly
            authorized -->
            <name>fax_send</name>
          </denied_operations>
          <operation>
            <name>net_delivery</name>
            <requirement>audit</requirement>
            242 ~ <requirement>explicit_authorization
              </requirement>
            ...
          </operation>
          <operation>
            ...
          </operation>
            243 ~ <allowed_operations> <!-- allowed without
              requirements -->
              <name>fax_receive</name>
              <name>store</name>
              ...
            </allowed_operations>
          </ace>
        <ace>
          ...
        </ace>
        ...
      </acl>
    </acc_rule>
    <acc_rule>
      <doc_category>ANY</doc_category>
      <doc_security_level>high</doc_security_level>
      <acl>
        ...
      </acl>
    </acc_rule>
  </policy>

```

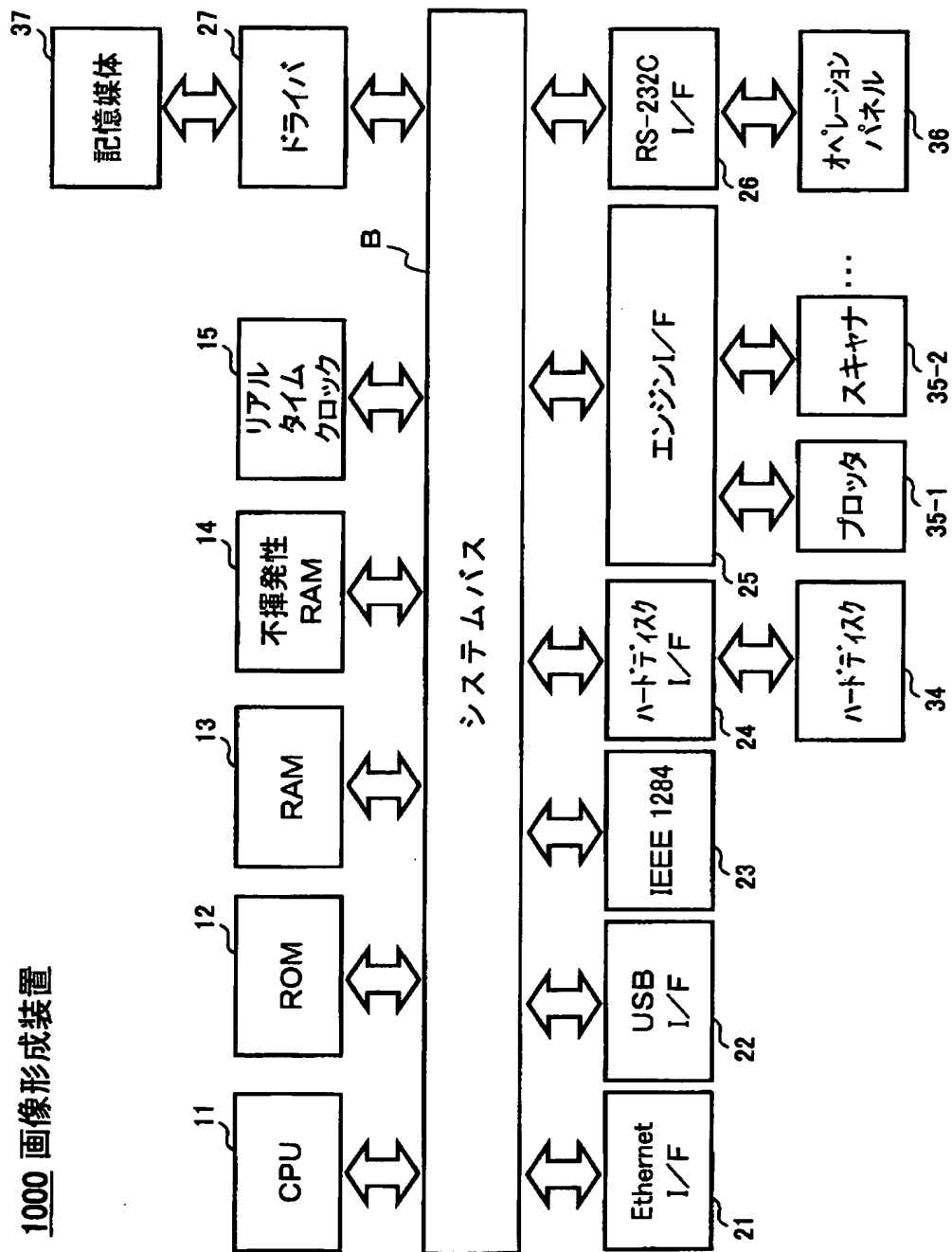
【図 26】

DSPを蓄積し且つ配布する種々の媒体を示す図



【図 27】

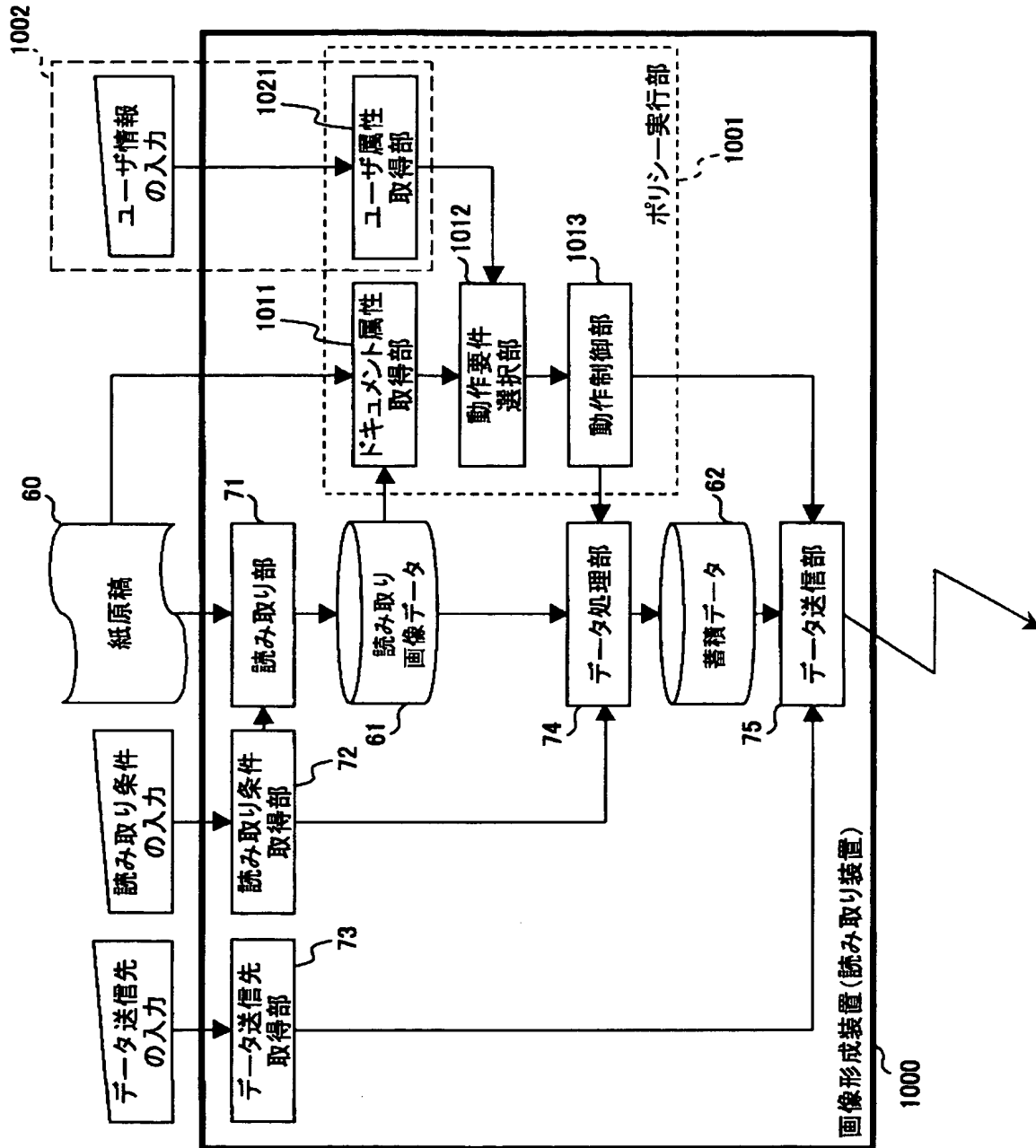
本発明の一実施例に係る画像形成装置の
ハードウェア構成を示すブロック図



1000 画像形成装置

【図 28】

セキュリティポリシーに従って動作する読み取り装置としての
画像形成装置の機能構成を示す図



【図 29】

簡略化したDSPの例を示す図

```

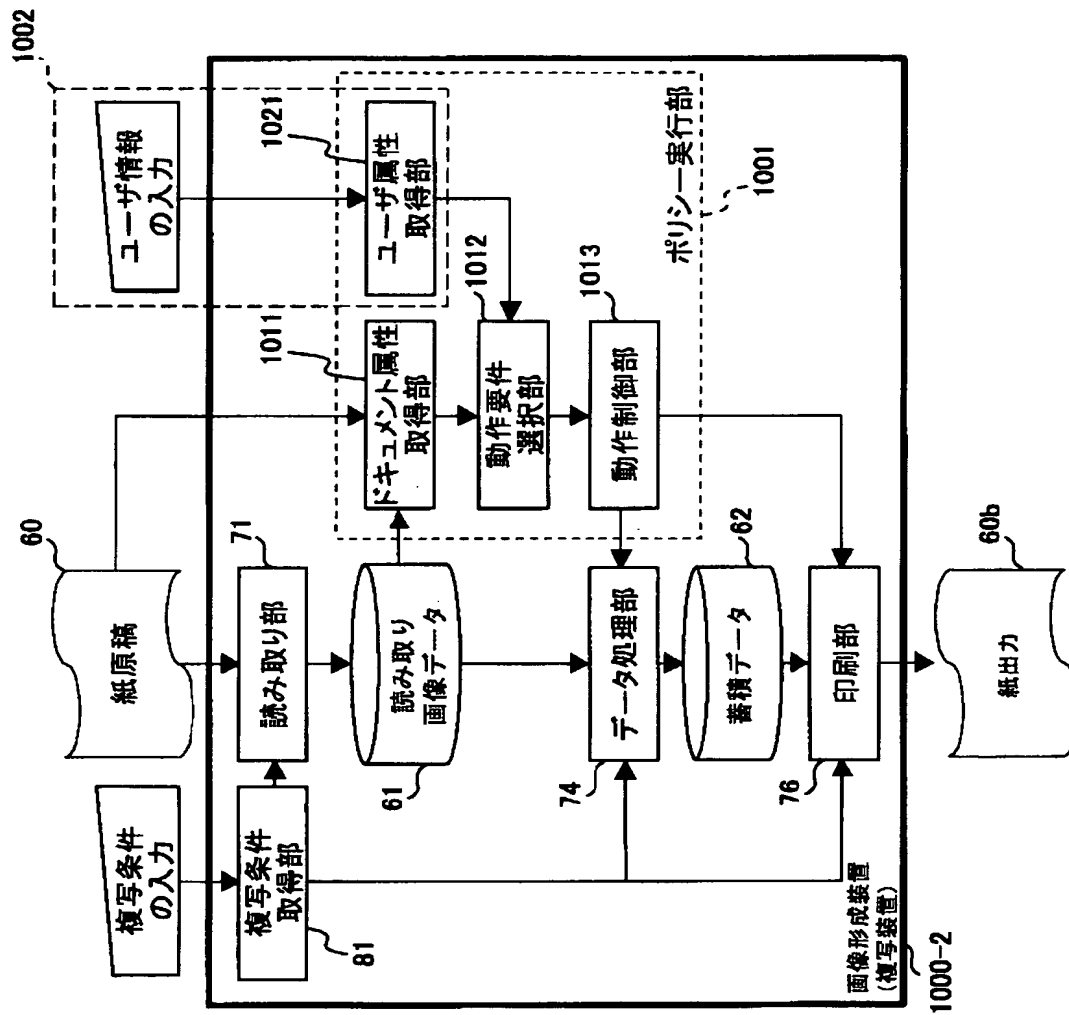
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>

```

2100

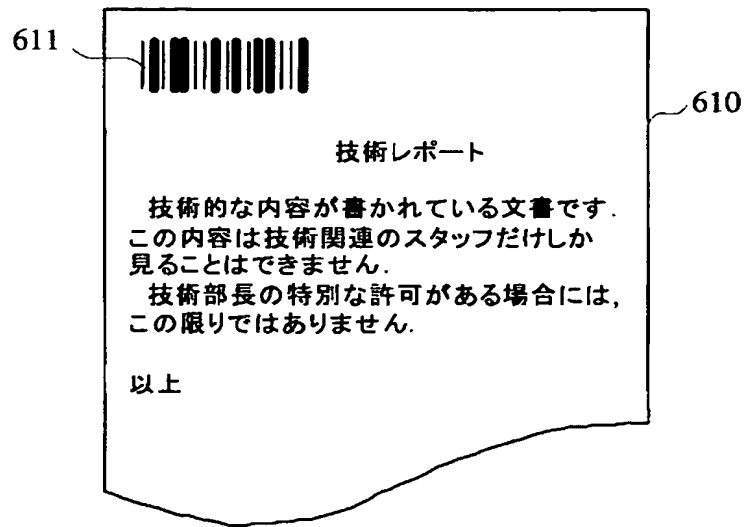
【図 30】

セキュリティポリシーに従って複写装置としての
画像形成装置の機能構成を示す図



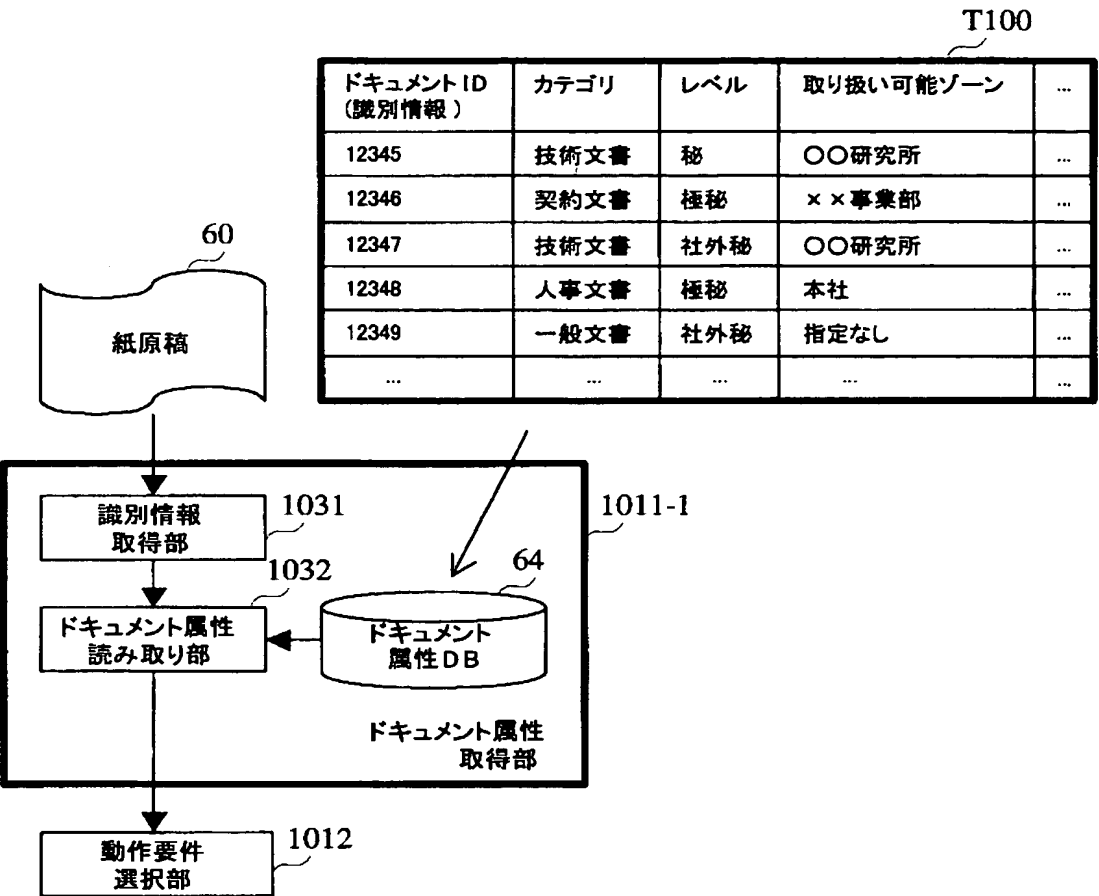
【図 31】

ドキュメントの識別情報をバーコードで印字した場合を示す図



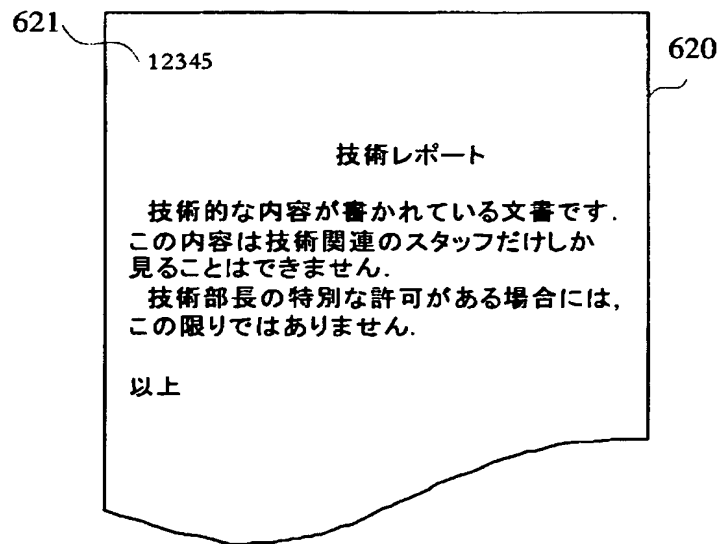
【図 3 2】

ドキュメント属性取得部の第1機能構成を示す図



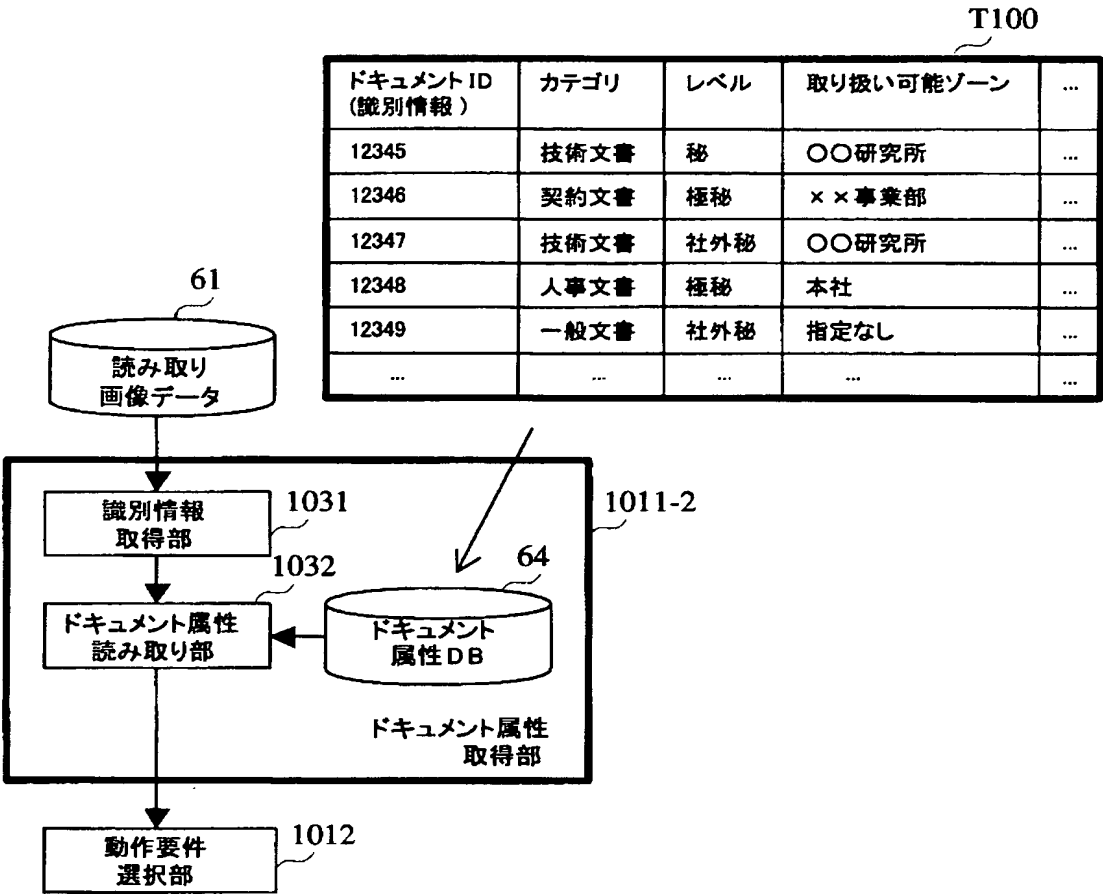
【図 33】

ドキュメントの識別情報を数字で印字した場合を示す図



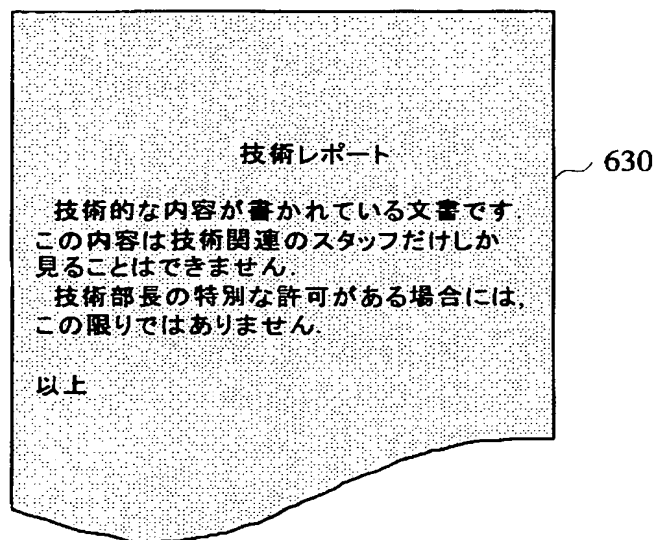
【図 3 4】

ドキュメント属性取得部の第2機能構成を示す図



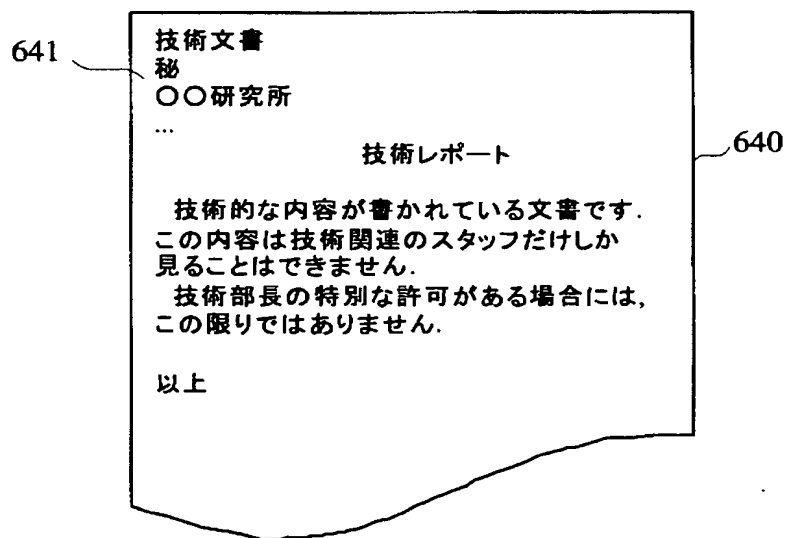
【図 35】

ドキュメントの識別情報を全面に印字した場合を示す図



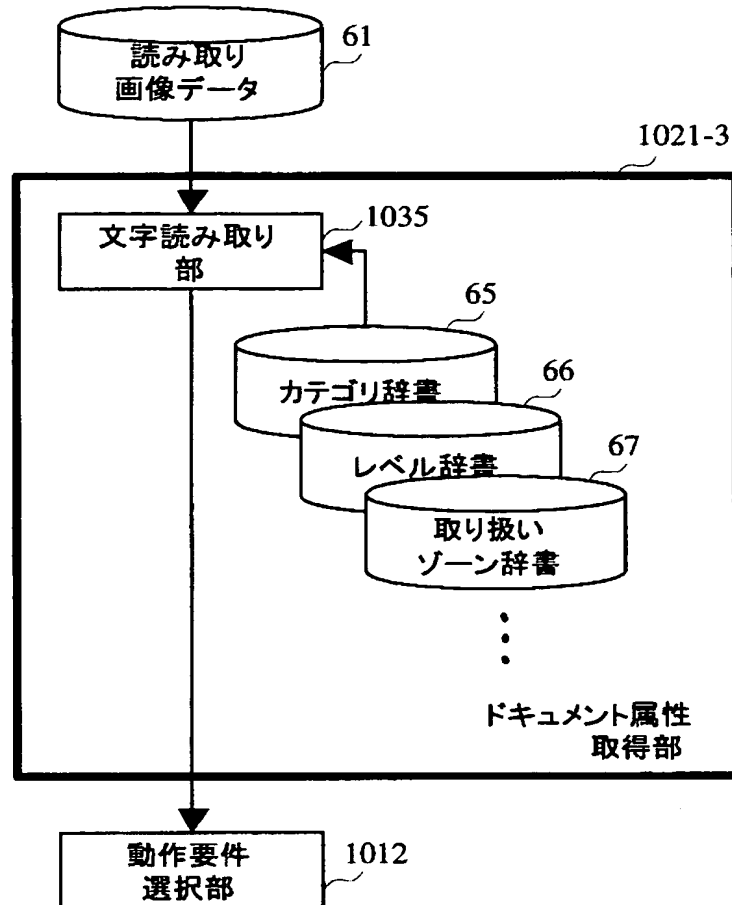
【図 36】

ドキュメントのセキュリティ属性を文字で印字した場合を示す図



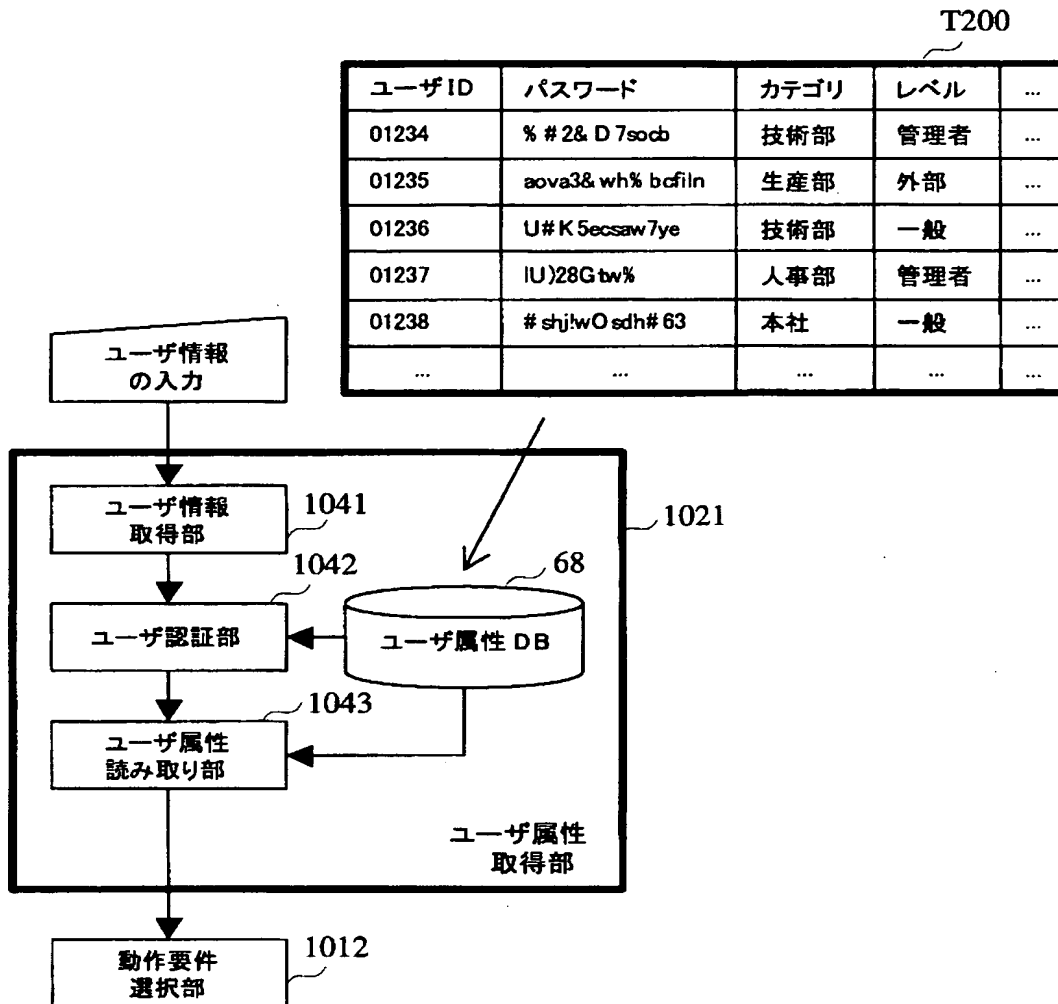
【図 37】

ドキュメント属性取得部の第3機能構成を示す図

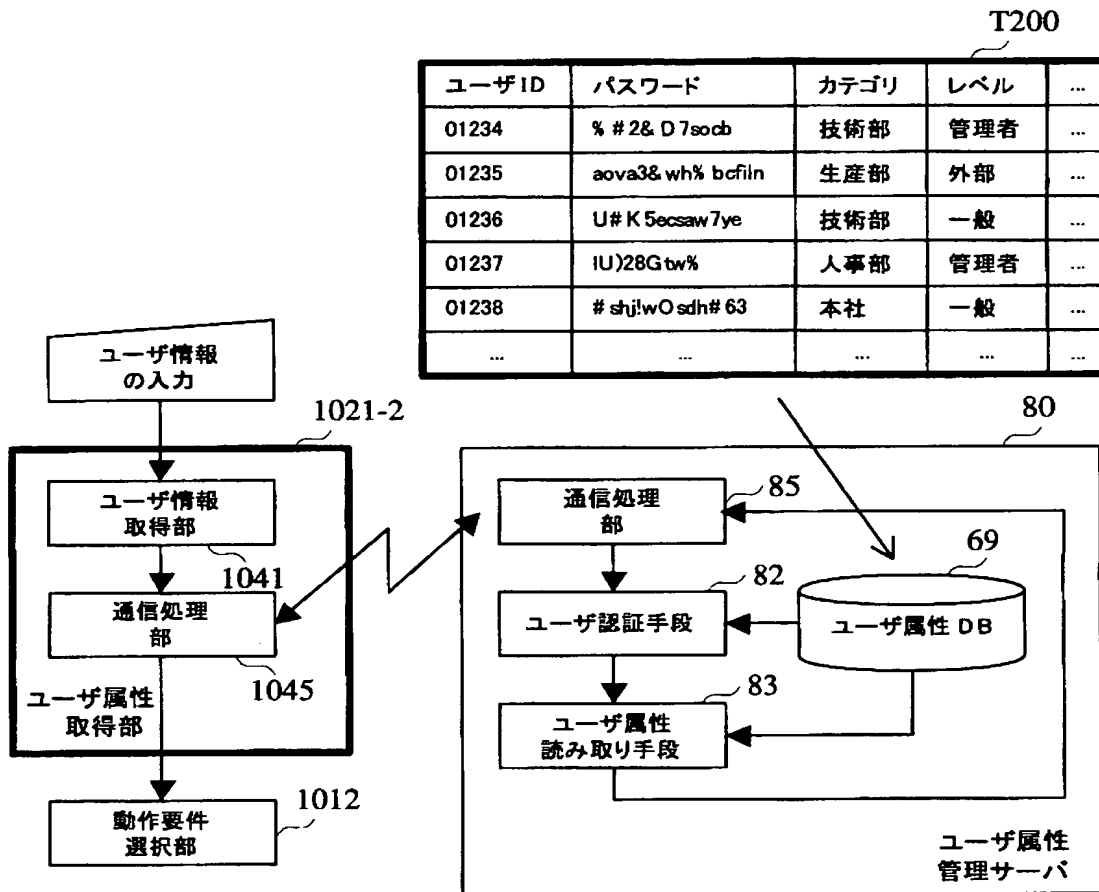


【図 38】

ユーザ属性取得部の機能構成を示す図



【図 39】

ユーザ属性を外部サーバから
取得する場合の機能構成を示す図

【書類名】 要約書**【要約】**

【課題】 本発明の課題は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいたドキュメントの読み取りとネットワーク配信を行う画像形成装置及び画像形成方法を提供することを目的とする。

【解決手段】 本発明の課題は、ドキュメントの識別情報を読み取る識別情報読取手段と、上記識別情報によって指定される動作要件を選択する動作要件選択手段と、上記動作要件選択手段によって選択された1つ以上の動作要件に従って所定動作の実行を制御する動作制御手段とを有する画像形成装置によって達成される。

【選択図】 図 2 8

特願 2 0 0 3 - 3 1 4 4 6 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 6 7 4 7]

1. 変更年月日

2 0 0 2 年 5 月 1 7 日

[変更理由]

住所変更

住 所

東京都大田区中馬込 1 丁目 3 番 6 号

氏 名

株式会社リコー